

VMware vCenter Configuration Manager Backup and Disaster Recovery Guide

vCenter Configuration Manager 5.4

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see <http://www.vmware.com/support/pubs>.

EN-000487-00

vmware[®]

You can find the most up-to-date technical documentation on the VMware Web site at:

<http://www.vmware.com/support/>

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

© 2006-2010 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About This Book	5
Implementing a Disaster Recovery Plan	7
Performing Backup Procedures	9
Backing Up the Database	9
Perform a Full Backup	10
Perform a Differential Backup	17
Perform a File System Backup	23
Back up HTTP Certificates	23
Performing Recovery Procedures	29
Import HTTP Certificates	30
Restoring the Databases	35
Restore the System Database	35
Restore the Report Server Database	37
Restore the VCM Databases	39
Installing VCM	41
Restoring File System Components	43
Script for Exported Reports	43
Index	45

About This Book

The *VCM Backup and Disaster Recovery Guide* describes the steps required to ensure the preparation and implementation of a successful disaster recovery plan for VMware vCenter Configuration Manager (VCM), and describes:

- Backup procedures
- Recovery procedures
- Database restoration procedures

Read this document and complete the procedures to prepare for a successful disaster recovery plan. The *VCM Backup and Disaster Recovery Guide* covers VCM version 5.3.

Intended Audience

The information presented in this manual is written experienced Windows and VCMsystem administrators.

To use this information effectively, you must have a basic understanding of how to configure network resources, install software, and administer operating systems. You also need to fully understand your network's topology and resource naming conventions.

Document Feedback

VMware welcomes your suggestions for improving our documentation. If you have comments, send your feedback to docfeedback@vmware.com.

VMware VCM Documentation

The vCenter Configuration Manager (VCM) documentation consists of the *VCM Hardware and Software Requirements Guide*, *VCM Installation and Getting Started Guide*, *VCM Foundation Checker User's Guide*, VCM online Help, and other associated documentation.

Technical Support and Education Resources

The following technical support resources are available to you. To access the current version of this book and other books, go to <http://www.vmware.com/support/pubs>.

- Online and Telephone Support** To use online support to submit technical support requests, view your product and contract information, and register your products, go to <http://www.vmware.com/support>. Customers with appropriate support contracts should use telephone support for priority 1 issues. Go to http://www.vmware.com/support/phone_support.html.
- Support Offerings** To find out how VMware support offerings can help meet your business needs, go to <http://www.vmware.com/support/services>.
- VMware Professional Services** VMware Education Services courses offer extensive hands-on labs, case study examples, and course materials designed to be used as on-the-job reference tools. Courses are available onsite, in the classroom, and live online. For onsite pilot programs and implementation best practices, VMware Consulting Services provides offerings to help you assess, plan, build, and manage your virtual environment. To access information about education classes, certification programs, and consulting services, go to <http://www.vmware.com/services>.

Implementing a Disaster Recovery Plan

To provide a disaster recovery plan for vCenter Configuration Manager (VCM), VMware recommends that you implement these procedures for an “Active Production / Standby Spare” recovery model.

This guide provides a baseline to configure the proper backup schedules and information on how to recover a system using these prepared backups. You may adjust the frequencies and retention values provided to meet specific service-level agreements and retention requirements.

When implementing a Disaster Recovery Plan, ensure the following:

- Historical data is retained. The data will be as current as the last scheduled database backup.
- Duplicate hardware of the production VCM Collector is available in an alternate location for recovery tasks.
- The recovery Collector is prepared with all software prerequisites for a VCM installation that matches the product versions of the production Collector.

Performing Backup Procedures

Use these procedures to ensure that all required databases have been properly backed up in compliance with your corporate standards. The maintenance plan created for this process should be used in addition to other database integrity and re-indexing maintenance plans. Although you may combine backup plans and other maintenance tasks into a single SQL Maintenance Plan, creating separate plans can assist in future troubleshooting and Maintenance Plan organization.

IMPORTANT Although the procedures in this document apply to SQL Server, you should apply the concepts about backing up your data to any third-party software you are using.

Backing Up the Database

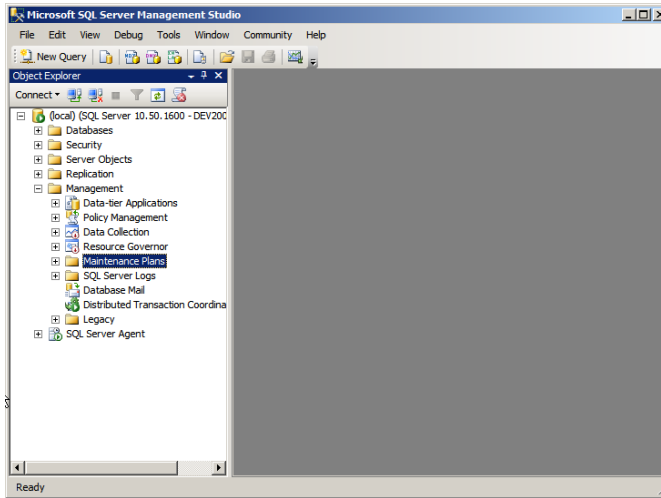
The example provided in this guide assumes a weekly full backup and a daily differential backup of each database. Transaction log (point-in-time) backups are not available because the VCM databases are configured in Simple Recovery mode, which is an advanced topic that is not covered in this document. For more information about Simple Recovery mode, see the SQL Server documentation.

Perform a Full Backup

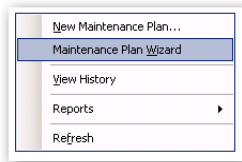
Full backups remain available on-disk for 28 days and differential backups remain available for 7 days. When adjusting the frequency or retention of backup schedules, ensure that the required amount of disk space is available for the maximum number of backup sets.

Procedure

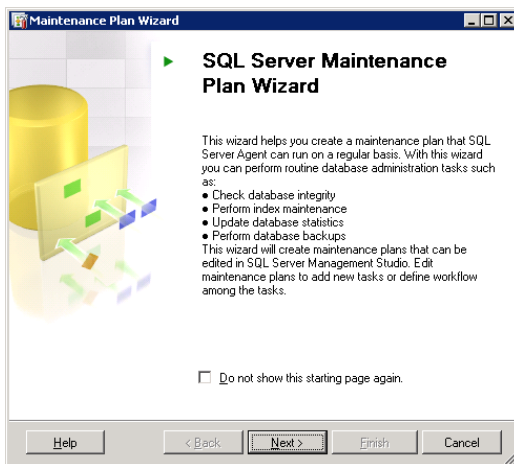
1. Select **Start > All Programs > Microsoft SQL Server 2008 R2 > SQL Server Management Studio**.
2. Connect to the VCM Database Server using an account with SQL Administrative privileges.



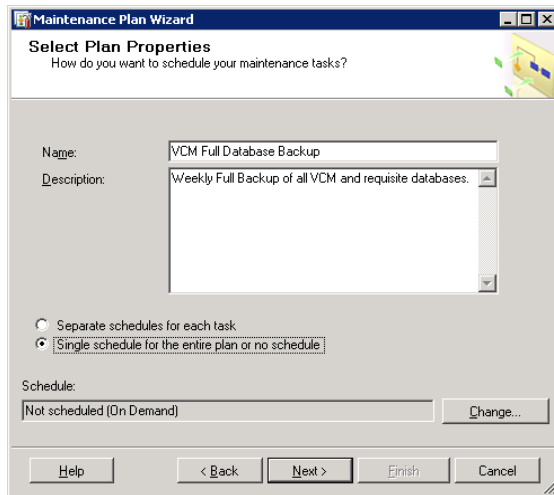
3. In Object Explorer, navigate to the Maintenance Plans node.



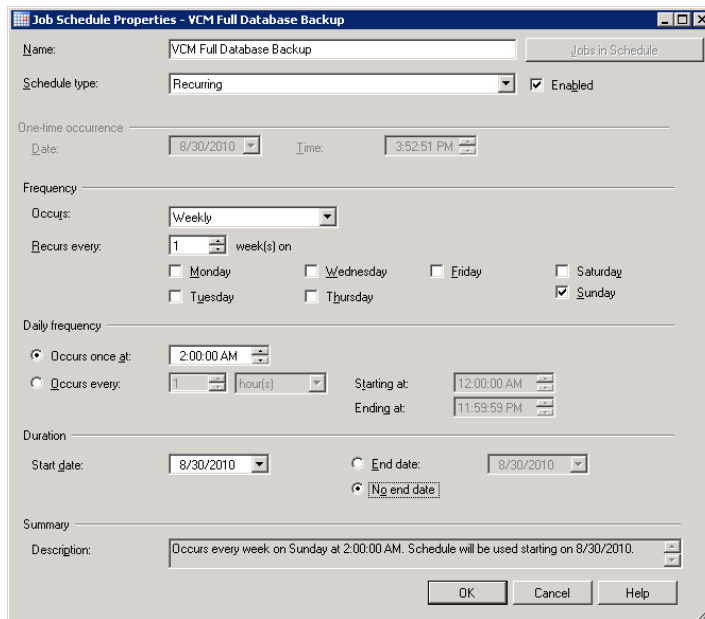
4. Right-click **Maintenance Plans**, and then select **Maintenance Plan Wizard**.



5. Click **Next**, and then enter a name and description for the maintenance plan.



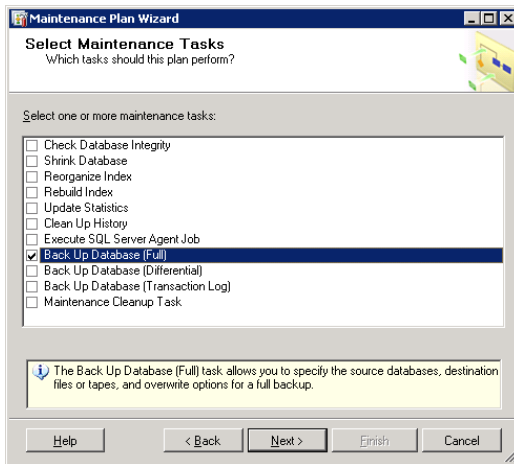
6. Click **Change** to create a schedule for the Full Backup Plan.



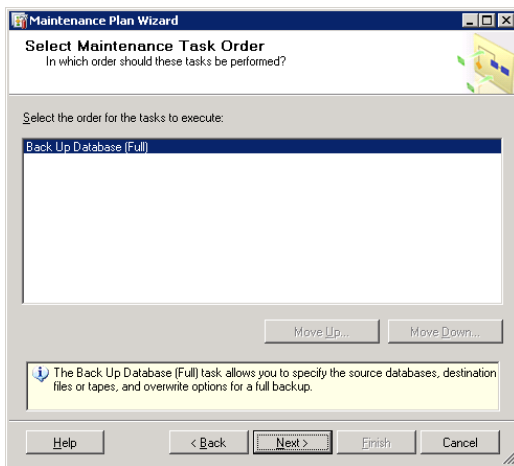
7. Ensure that the schedule is enabled as a **Recurring** schedule type.

Back up regularly. Depending on your corporate policy, you may need to back up daily rather than weekly.

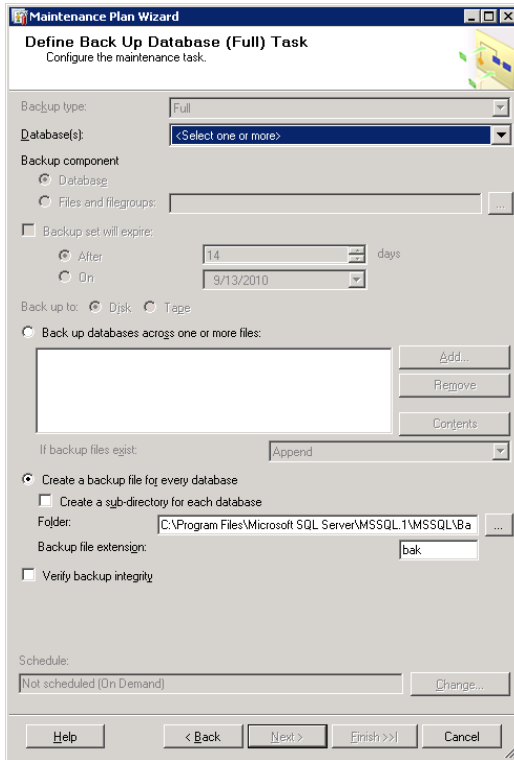
8. Configure the schedule at a time when minimal Collector activity will be occurring, and click **OK** and then **Next**.



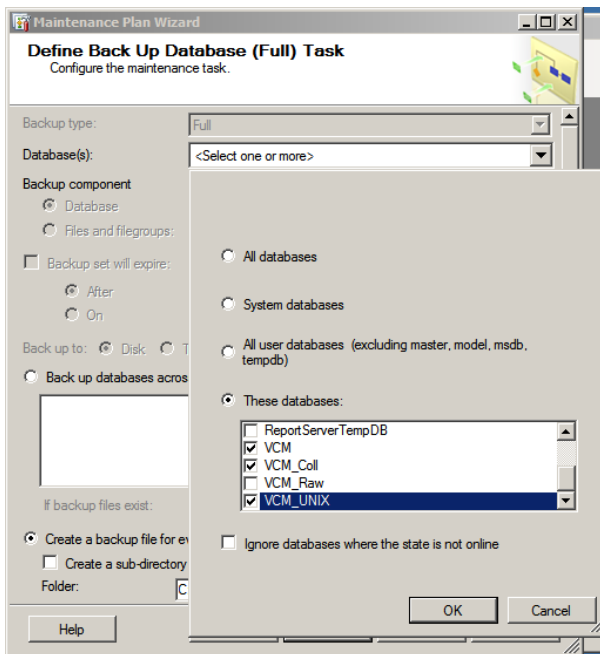
9. On the Select Maintenance Tasks page, select **Back Up Database (Full)** and click **Next**.



10. On the Select Maintenance Task Order page, if you are combining this backup task with other tasks, set an appropriate execution order and place the backup task after all the other tasks.

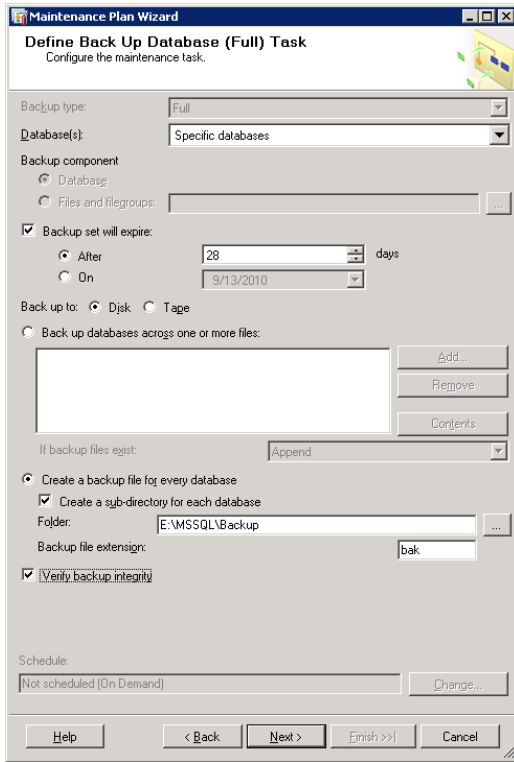


- On the Define Back Up Database (Full) Task page, click the **Database(s)** drop-down menu and select the databases to back up.

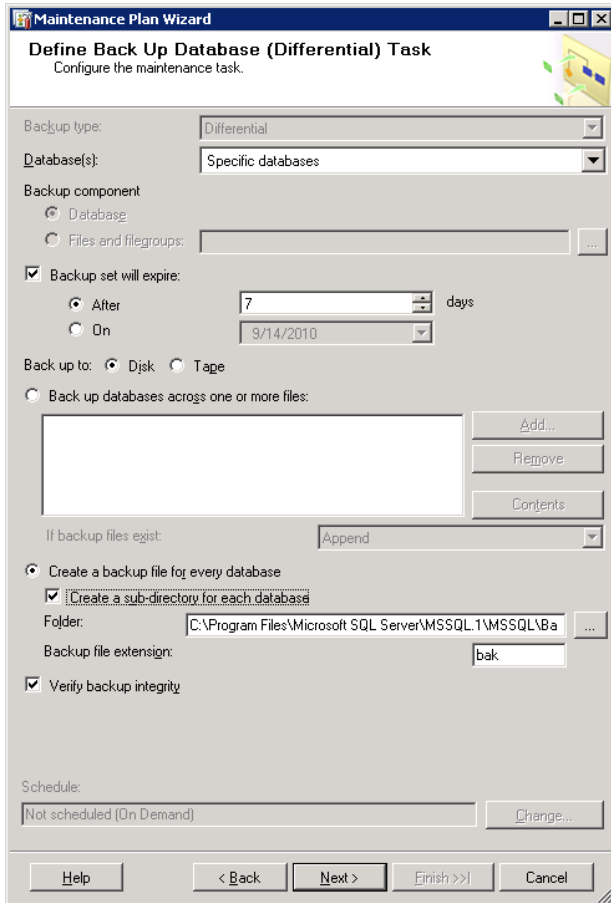


Include these databases in the backup set: **CSI_Domain**, **master**, **msdb**, **ReportServer**, **VCM**, **VCM_Coll**, and **VCM_UNIX**. If alternate names were used during the initial installation, select the corresponding databases.

- Click **OK** to select the databases and return to the Define Back Up Database (Full) Task.

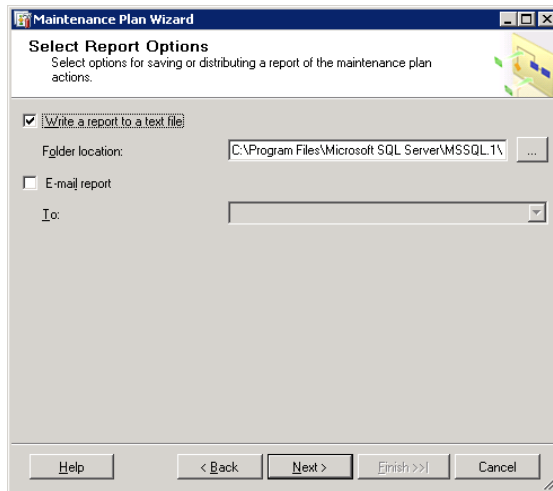


13. Click **OK** to select the databases and return to the Define Back Up Database (Full) Task.

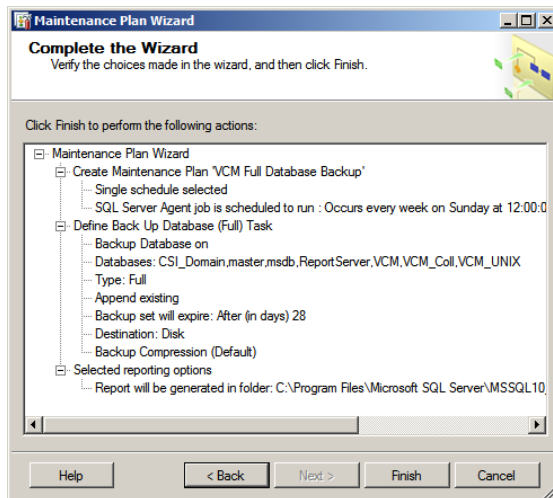


Configure the additional settings:

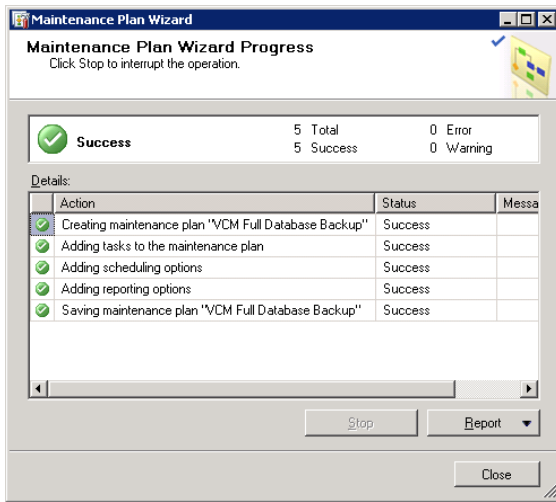
- **Backup set will expire:** Specify **After 28 days**. Depending on your corporate backup policies and disk space available, you might need to modify this setting to match your policy.
 - **Back up to:** Select **Disk**.
 - **Create a backup file for every database:** Select this option and **Create a sub-directory for each database**. Then specify the folder for the designated backup drive and folder structure.
 - **Backup file extension:** Specify the extension as **bak**.
 - **Verify backup integrity:** Select this option.
14. Click **Next** and on the Select Report Options page make sure **Write a report to text file** is selected and a folder location is specified.



15. On the Complete the Wizard page, verify all of the selected options are correct.



16. Click **Finish** to complete the maintenance plan.



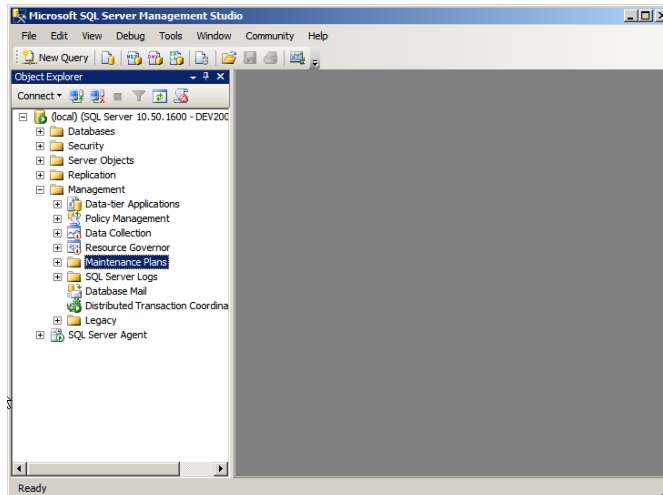
17. Ensure all tasks complete successfully.

Perform a Differential Backup

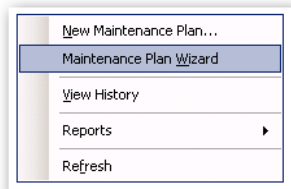
You should perform a daily, differential backup.

Procedure

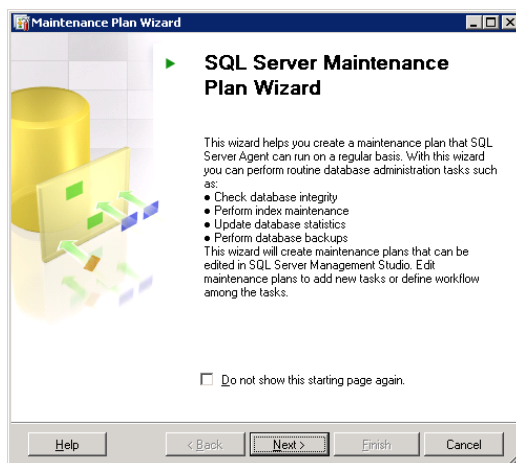
1. Select **Start > All Programs > Microsoft SQL Server 2008 R2 > SQL Server Management Studio**.
2. Connect to the VCM Database Server using an account with SQL Administrative privileges.



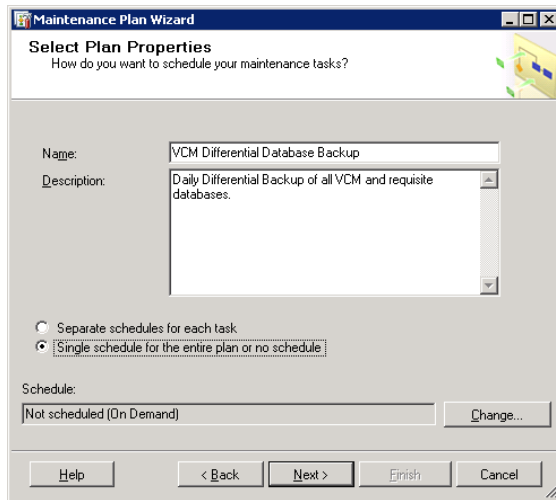
3. Navigate to the Maintenance Plans node in the Object Explorer.



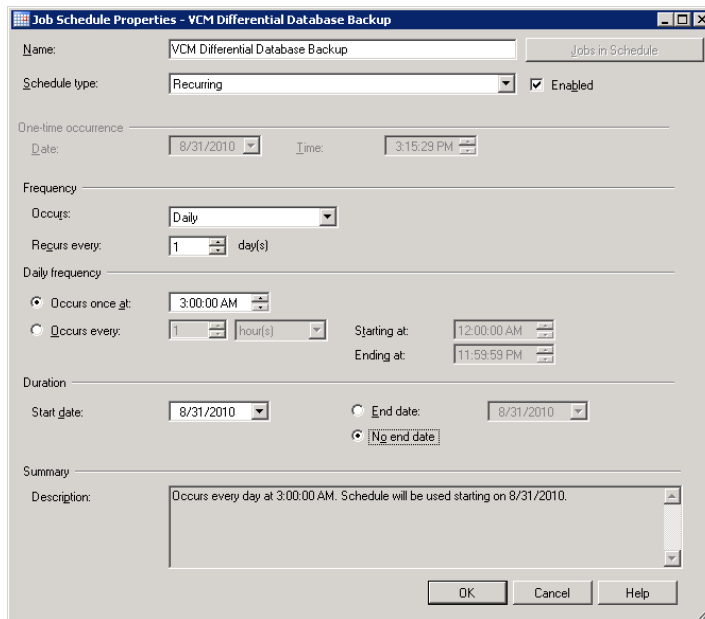
4. Right-click **Maintenance Plans** and select **Maintenance Plan Wizard**.



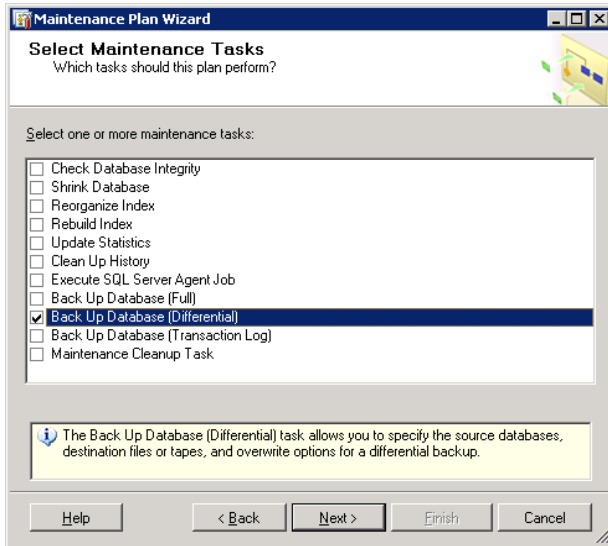
5. Click **Next**, and then enter a name and description for the maintenance plan.



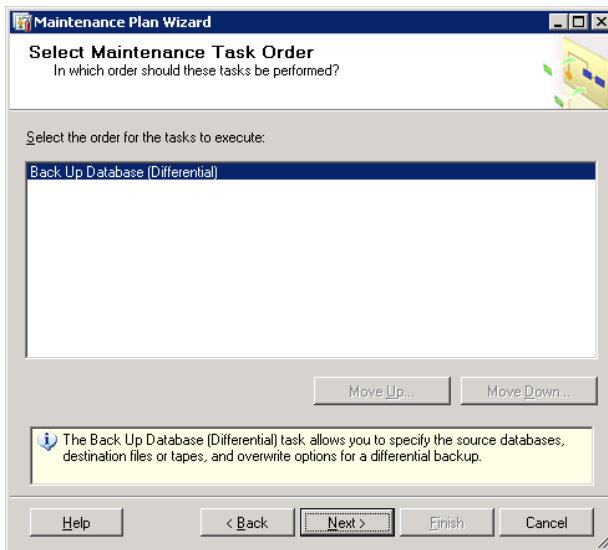
6. Click **Change** to create a schedule for the Differential Backup Plan.



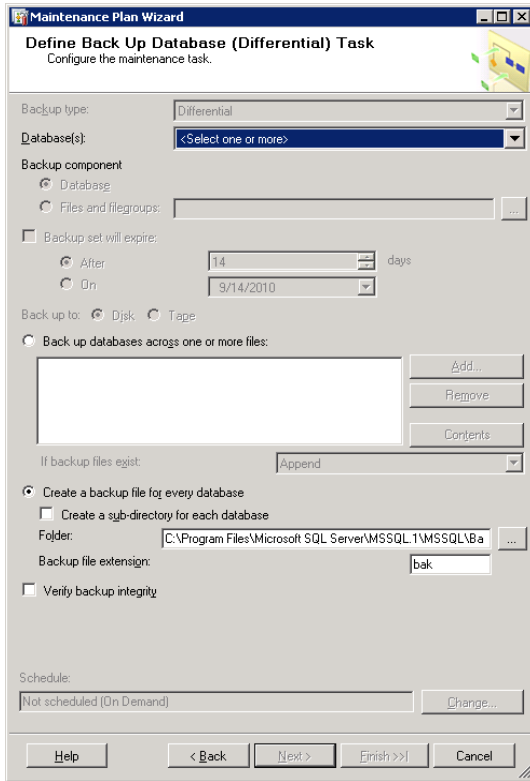
7. Ensure that the schedule is enabled as a **Recurring** schedule type.
Back up regularly. Depending on your corporate policy, you may need to back up daily rather than weekly.
8. Configure the schedule at a time when minimal Collector activity will be occurring, and click **OK** and then **Next**.



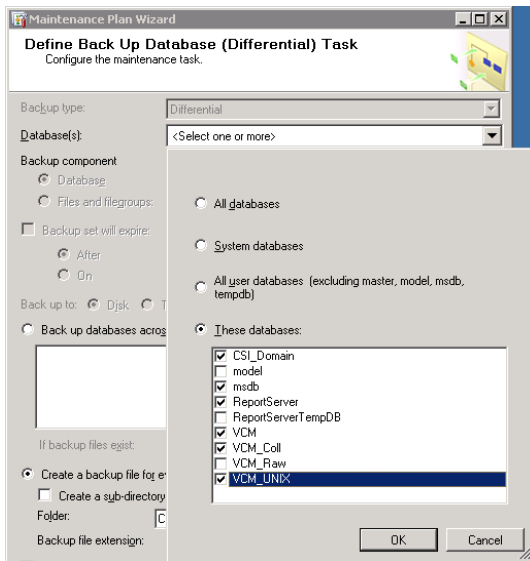
9. On the Select Maintenance Tasks page, select **Back Up Database (Differential)** and click **Next**.



10. On the Select Maintenance Task Order page, if you are combining this backup task with other tasks, set an appropriate execution order and place the backup task after all the other tasks.



11. On the Define Back Up Database (Differential) Task page, click the **Database(s)** drop-down menu and select the databases to be backed up.

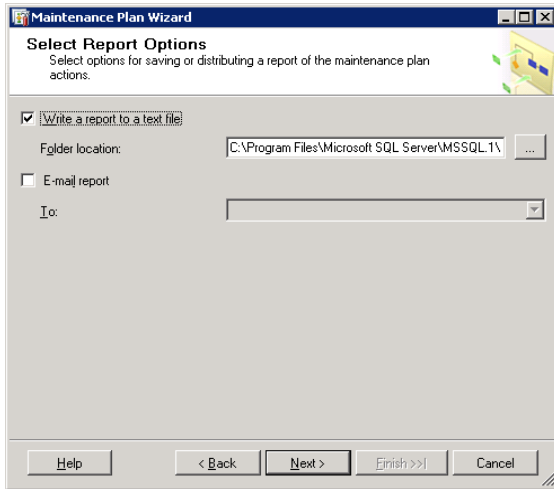


Include these databases in the backup set: **CSI_Domain**, **msdb**, **ReportServer**, **VCM**, **VCM_Coll**, and **VCM_UNIX**. If alternate names were used during the initial installation, select the corresponding databases.

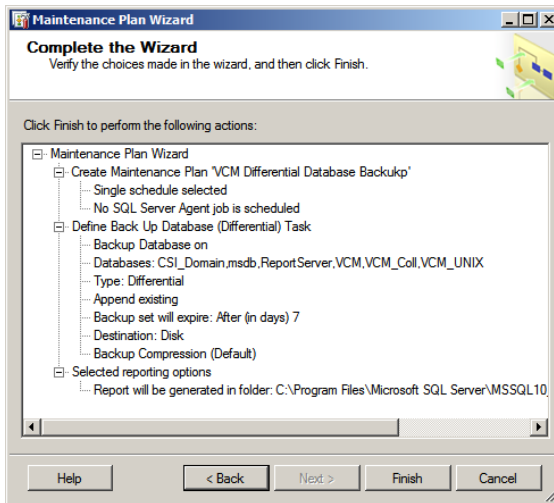
12. Click **OK** to select the databases and return to the Define Back Up Database (Differential) Task.

Configure the additional settings:

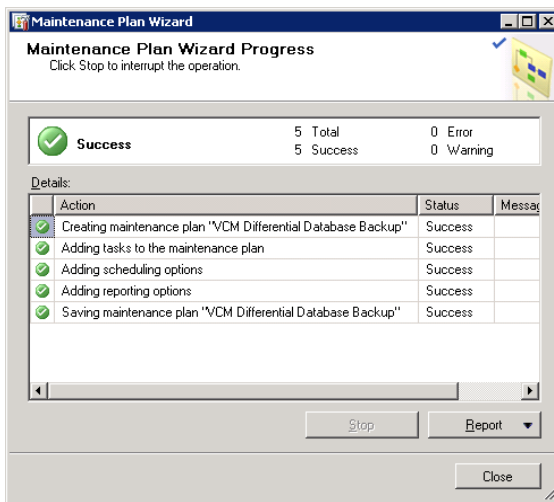
- **Backup set will expire:** Specify **After 7 days**. Depending on your corporate backup policies, you might need to modify this setting to match your policy.
 - **Back up to:** Select **Disk**.
 - **Create a backup file for every database:** Select this option and **Create a sub-directory for each database**. Then specify the folder for the designated backup drive and folder structure.
 - **Backup file extension:** Specify the extension as **bak**.
 - **Verify backup integrity:** Select this option.
13. Click **Next** and on the **Select Report Options** page make sure **Write a report to text file** is selected and a folder location is specified.



- On the Complete the Wizard page, verify all of the selected options are correct.



- Click **Finish** to complete the maintenance plan.



- Ensure all tasks complete successfully.

Perform a File System Backup

You may perform file system backups using corporate standard tools or simple scripted file copies. It is not necessary to back up the entire file system or the VCM Program directory structure.

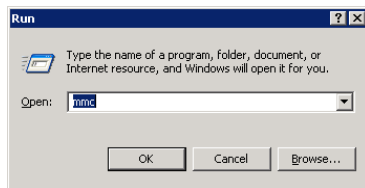
At a minimum, create a backup of the entire content of the `CMFILES$` share at the default location of `C:\Program Files (x86)\VMware\VCM\WebConsole\L1033\Files`. If customizations have been made to your Collector, or if reports have been exported to a non-default location, you must also ensure that these additional files are backed up as needed.

Back up HTTP Certificates

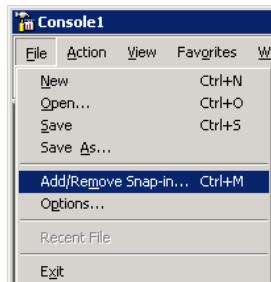
If HTTP Agents are in use, you must ensure that your HTTP Certificates are available for disaster recovery purposes. The certificates must only be exported once for each new server and maintained in a secure location for disaster recovery purposes.

Procedure

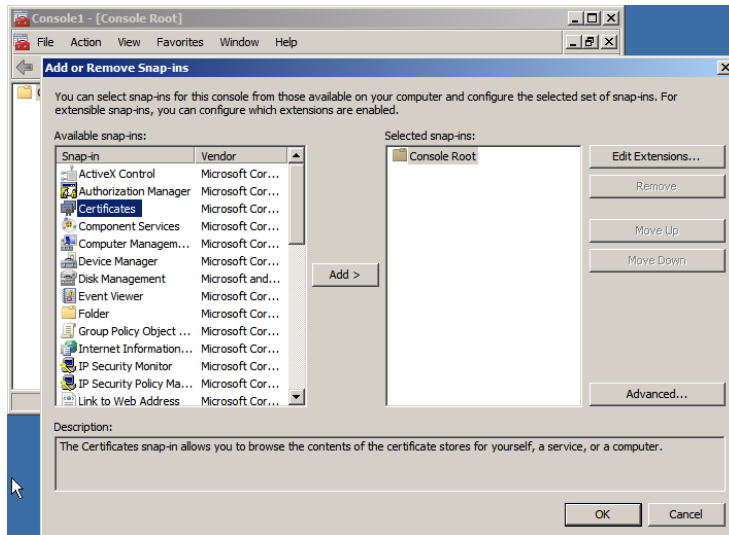
1. On the Collector server, click **Start > Run**.



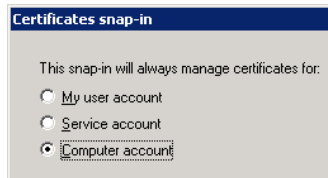
2. Enter `mmc` to start the Microsoft Management Console.



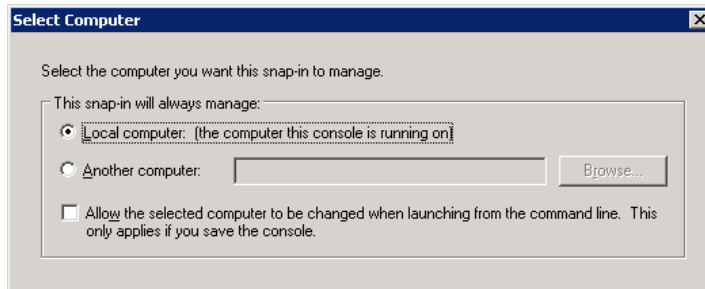
3. From the **File** menu, select **Add/Remove Snap-in** to add a new Snap-in.



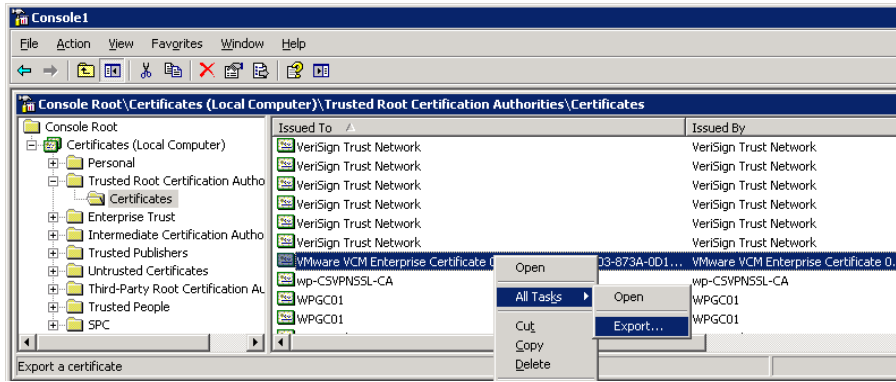
4. In the Add or Remove Snap-ins window, select **Certificates** and click **Add >**.



5. In the Certificates snap-in window, select **Computer account** to manage certificates for a computer account and click **Next**.



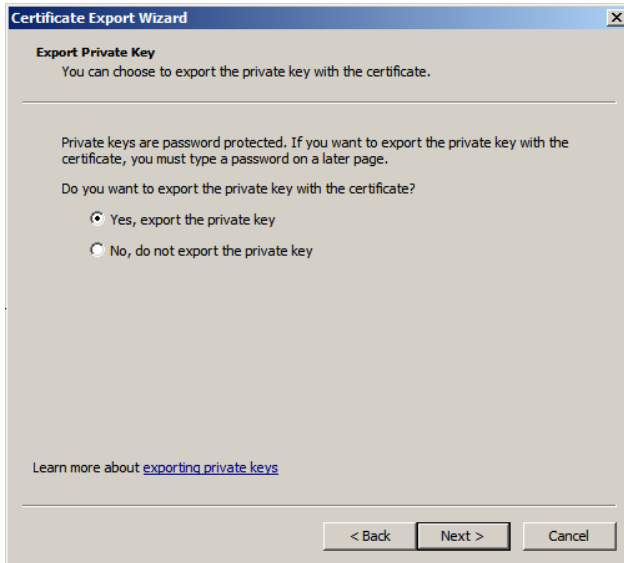
6. In the Select Computer window, select **Local computer** for the snap-in to manage certificates on the local computer and click **Finish**.
7. Click **OK** to close the Add or Remove Snap-ins window and return to the Console.
8. From the Console Root, navigate to **Trusted Root Certification Authorities** and click **Certificates**.



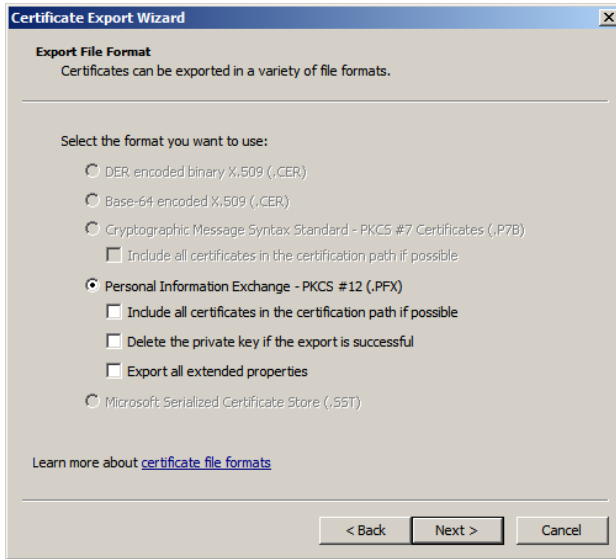
9. Right-click VMware VCM Enterprise Certificate and select All Tasks > Export.



10. On the Certificate Export Wizard Welcome page, click Next.



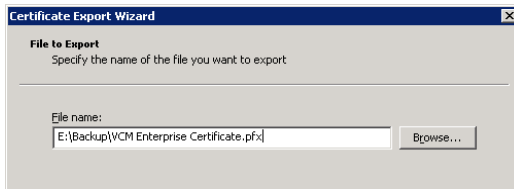
11. On the Export Private Key page, select to export the private key with the certificate and click Next.



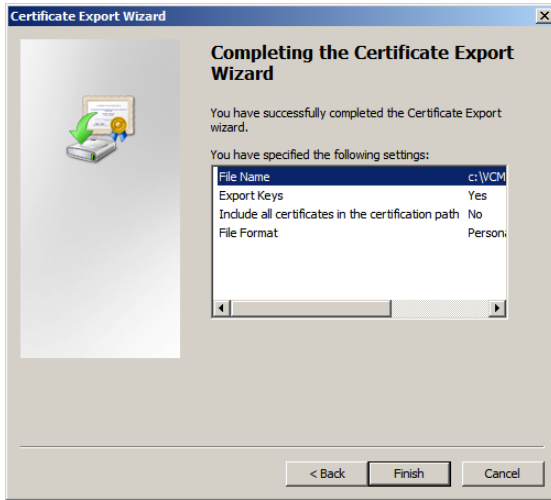
12. Accept the Personal Information Exchange default setting and click **Next**.



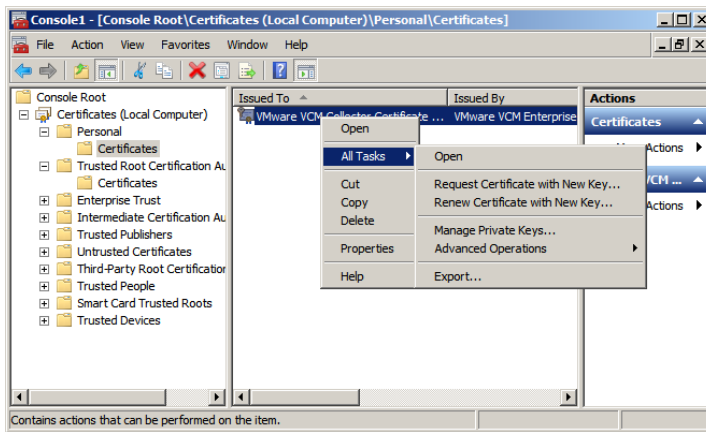
13. Enter a password for the certificate export and click **Next**.



14. Enter a location and name for the VMware VCM Enterprise Certificate.



15. Verify your selected options and click **Finish** to complete the export process. The Certificate Export Wizard reports the export was successful. Click **OK** to close the Certificate Export Wizard window.
16. Expand **Personal > Certificates** and locate your Personal Certificate.



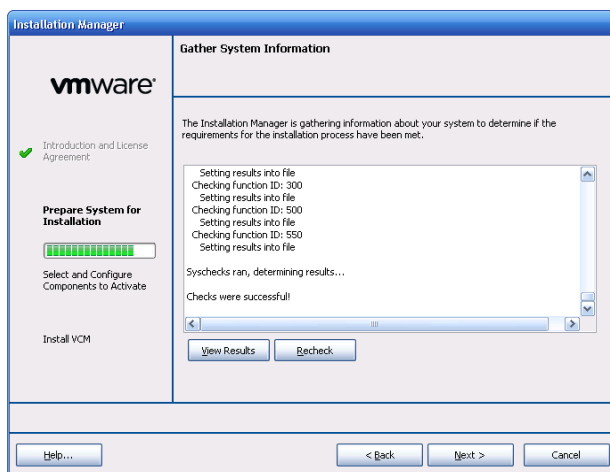
17. Right-click the Personal Collector Certificate and select **All Tasks > Export** to use the VMware VCM Collector Certificate as the Personal Certificate to export.

Performing Recovery Procedures

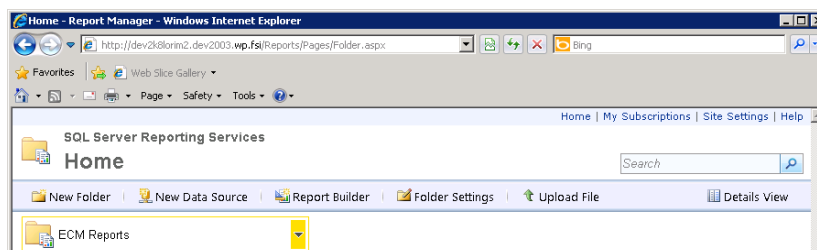
You must verify that the prerequisites check completed successfully and that the SSRS Report folder is accessible.

Procedure

1. Use the *VCM 5.4 Installation and Getting Started Guide* to install and validate all VCM prerequisites on the recovery server.



2. Ensure the prerequisites check completed successfully.
3. Open Internet Explorer and navigate to `http://[SERVERNAME]/reports`, where `SERVERNAME` is the name of the recovery server.



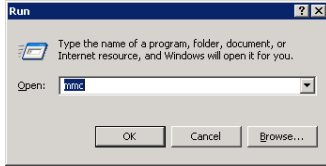
4. Ensure that **ECM Reports** appears.

Import HTTP Certificates

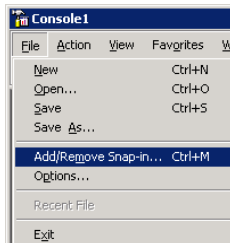
You must add the Certificate snap-in to the Microsoft Management Console.

Procedure

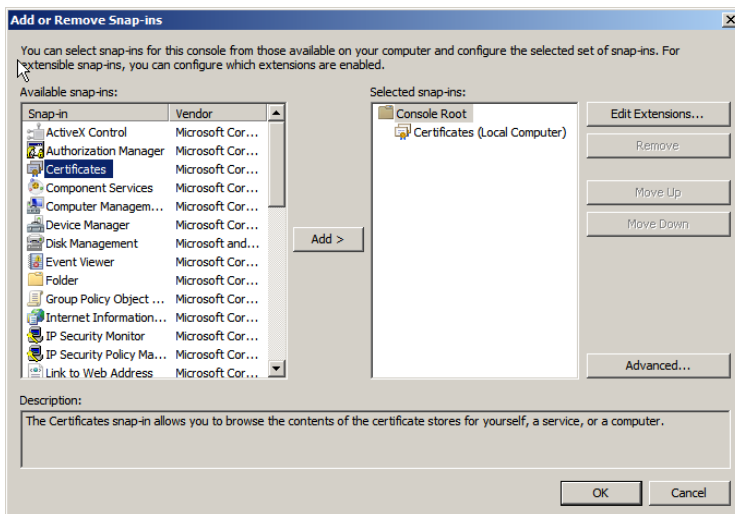
1. On the Collector server, click **Start > Run**.



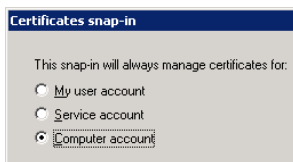
2. Enter **mmc** to start the Microsoft Management Console.



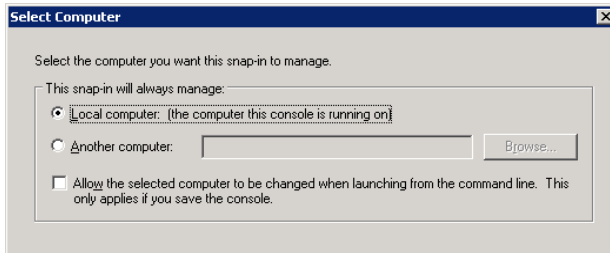
3. From the File menu, select **Add/Remove Snap-in** to add a new Snap-in.



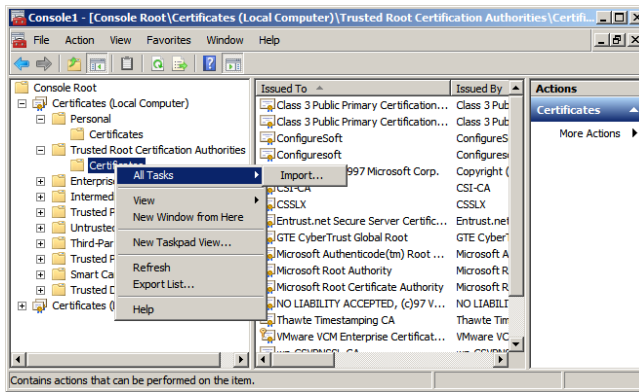
4. In the Add or Remove Snap-ins window, select **Certificates** and click **Add >**.



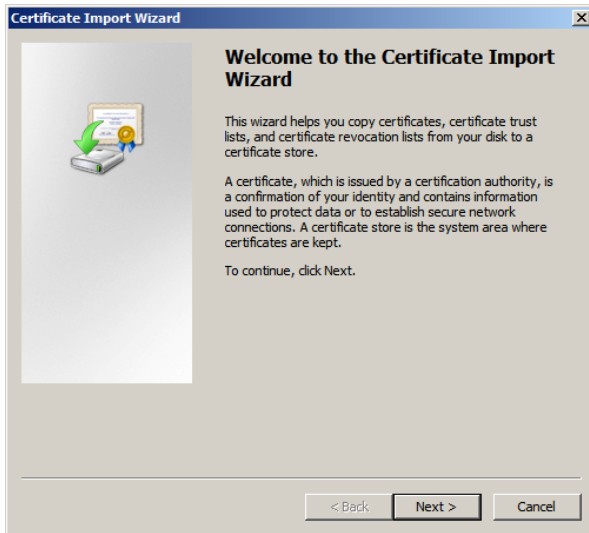
5. In the Certificates snap-in window, select **Computer account** to manage certificates for a computer account and click **Next**.



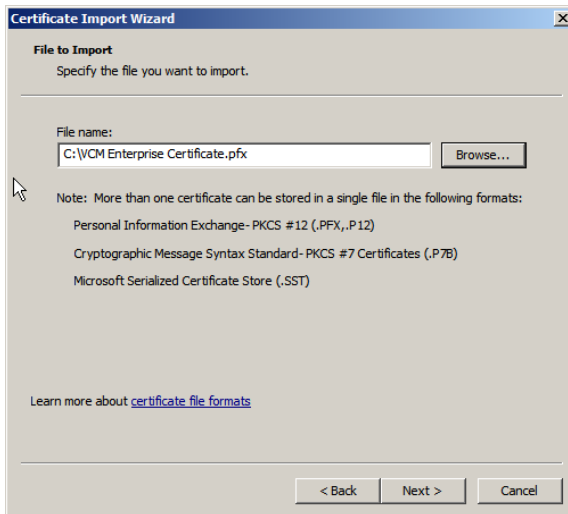
6. In the Select Computer window, select **Local computer** for the snap-in to manage certificates on the local computer and click **Finish**.
7. Click **OK** to close the Add or Remove Snap-ins window and return to the Console.
8. Locate the **Trusted Root Certification Authorities** and the **Certificates** store.



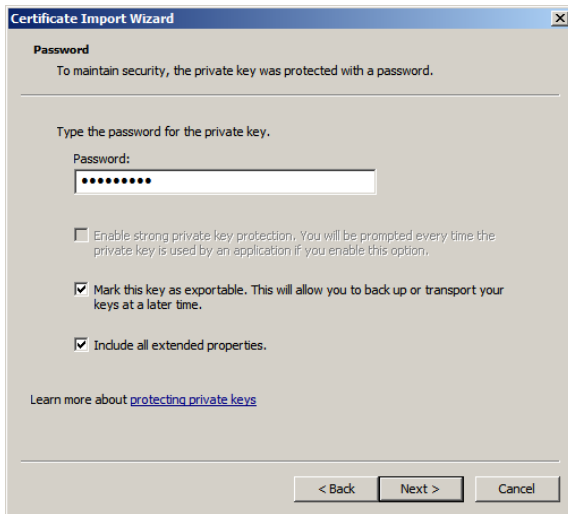
9. Right-click **Certificates**, select **All Tasks > Import**.



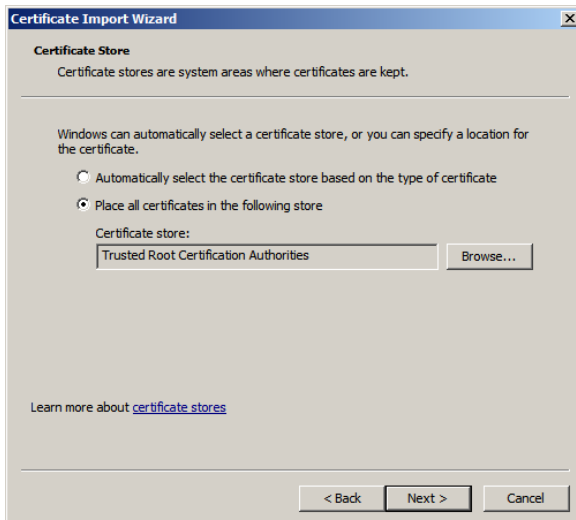
10. On the Certificate Export Wizard Welcome page, click **Next**.



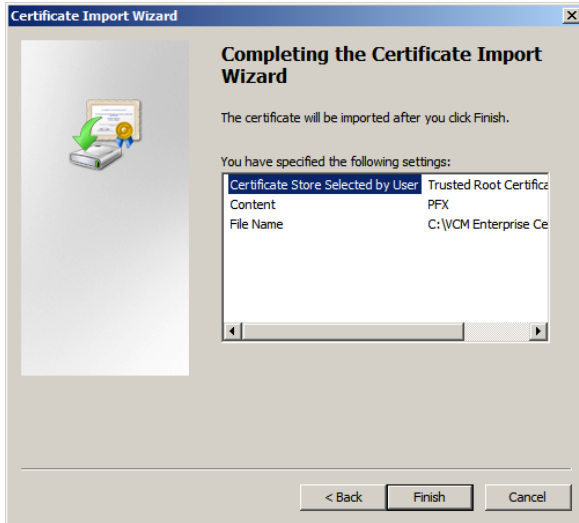
11. Locate and select the VCM Enterprise Certificate from the production system.



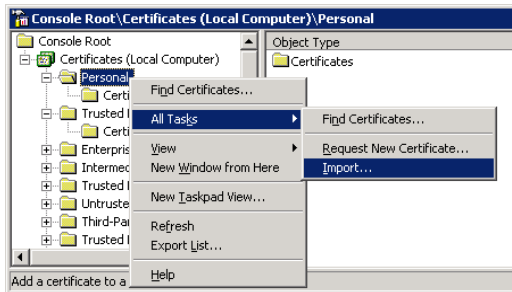
12. Enter the required password, verify the "Mark this key as exportable" check box is selected and click **Next**.



13. Select to place all certificates in the Trusted Root Certification Authorities store and click **Next**.



14. Verify your selected options and click **Finish** to complete the import process. The Certificate Import Wizard reports the import was successful. Click **OK** to close the Certificate Import Wizard window.
15. Expand **Personal > Certificates** and locate your Personal Certificate.



16. Right-click the Personal Collector Certificate and select **All Tasks > Import** to import the VCM Collector Certificate into the Personal certificate store.

Restoring the Databases

Database restoration must occur in three phases and in the proper order. First, to restore proper user access and scheduled jobs, the system database is restored. Next, to recover SQL Reporting Services, the SQL Report Server databases is restored. Finally, the VCM Database is restored.

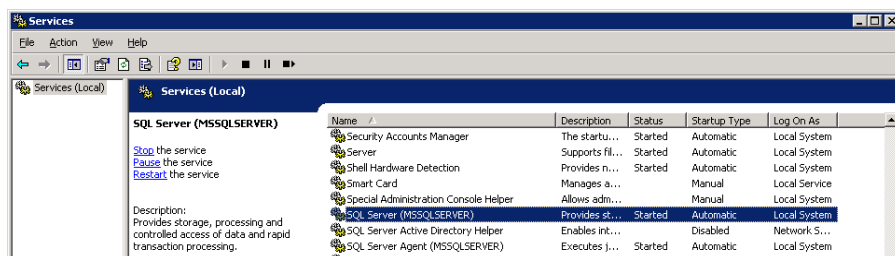
Restore the System Database

You must take extra steps to properly restore the system databases. To restore the master database, you must first place the SQL Server in single-user mode. After the master database has been restored, you must run a command to update the SQL Server name.

You must be an Administrator to start and stop the SQL Server services.

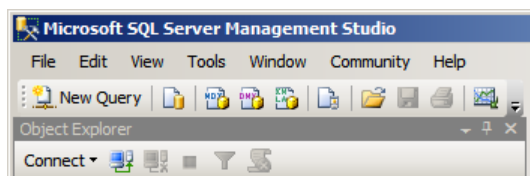
Procedure

1. Place the SQL Server in Single-user Mode by selecting **Start > Administrative Tools > Services**.

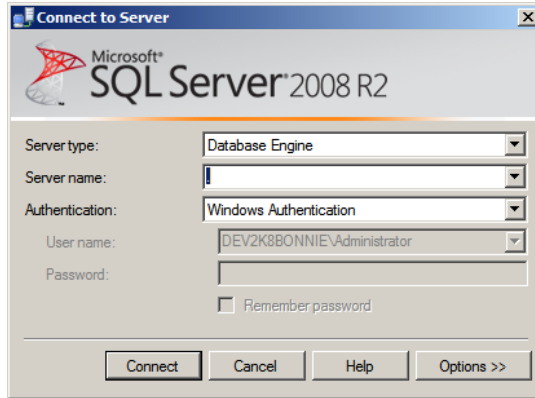


2. Right-click the SQL Server (MSSQLSERVER) service and select **Stop**.
3. If you are prompted to stop other services, such as the SQL Server Agent, select **Yes** and wait for the service to stop.
4. Start the SQL Server service in single-user mode in a command window by entering:


```
NET START MSSQLSERVER /c /m
```
5. Wait for the service to start successfully.
6. Start SQL Server Management Studio.
7. When you are prompted for login credentials, select **Cancel** to avoid opening the Object Explorer.



8. Click **New Query** to start a new query definition.



9. Log into the SQL Server with the local SQL account.
10. In the query window, enter the command to restore the MASTER Database from backup:

```
USE MASTER
GO
RESTORE DATABASE [master]
FROM DISK = N'E:\MSSQL\Backup\master\master_backup_201003021337.bak'
WITH FILE=1, NOUNLOAD, REPLACE, STATS = 10
GO
```

11. Click **Execute** and wait for SQL Server to restart and display the message:

```
The master database has been successfully restored. Shutting down SQL Server.
SQL Server is terminating this process.
```

12. Select **New Query** to reconnect to the SQL server using Administrative privileges and the local account or Windows Authentication.
13. Rename the SQL Server @@servername definition with the command:

```
USE master
GO
DECLARE @NewServerName varchar(254)
SET @NewServerName = Convert(varchar(254), serverproperty ('ServerName'))
EXEC sp_dropserver @@servername
EXEC sp_addserver @NewServerName, local
GO
```

14. Click **Execute**.
15. Restart the SQL Server Service and reconnect using an account with Administrative privileges.
16. Restore the **msdb** database with the command:

```
RESTORE DATABASE [msdb]
FROM DISK = N'E:\Backup\msdb\msdb_backup_201003021337.bak'
WITH FILE=1, NOUNLOAD, REPLACE, STATS = 10
GO
```

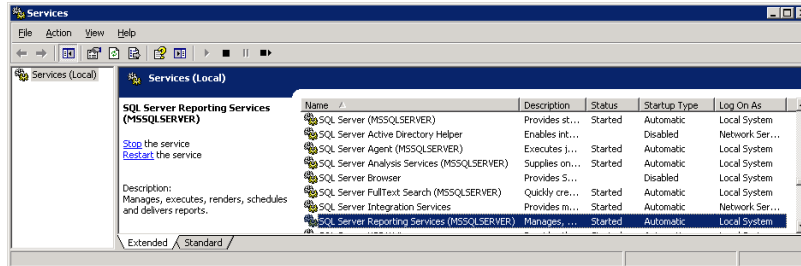
17. Click **Execute**.

Restore the Report Server Database

To recover SQL Reporting Services, you must next restore the SQL Report Server databases.

Procedure

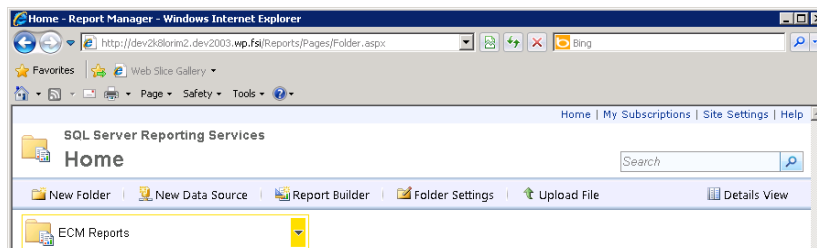
1. Stop the SQL Server Reporting Services service by selecting **Start > Administrative Tools > Services**.



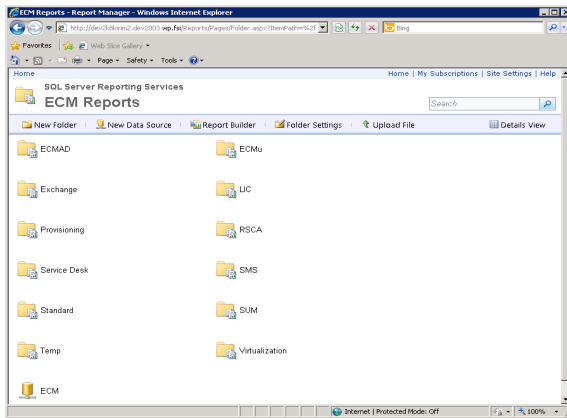
2. Right-click the **SQL Server Reporting Services (MSSQLSERVER)** service and select **Stop**.
3. Stop Internet Information Services (IIS) with the `iisreset /stop` command and wait for the services to stop.
4. Restore the ReportServer Database from SQL Management Studio.

```
RESTORE DATABASE [ReportServer]
FROM DISK = N'E:\Backup\ReportServer\ReportServer_backup_201003021337.bak'
WITH FILE=1, NOUNLOAD, REPLACE, STATS = 10
GO
```

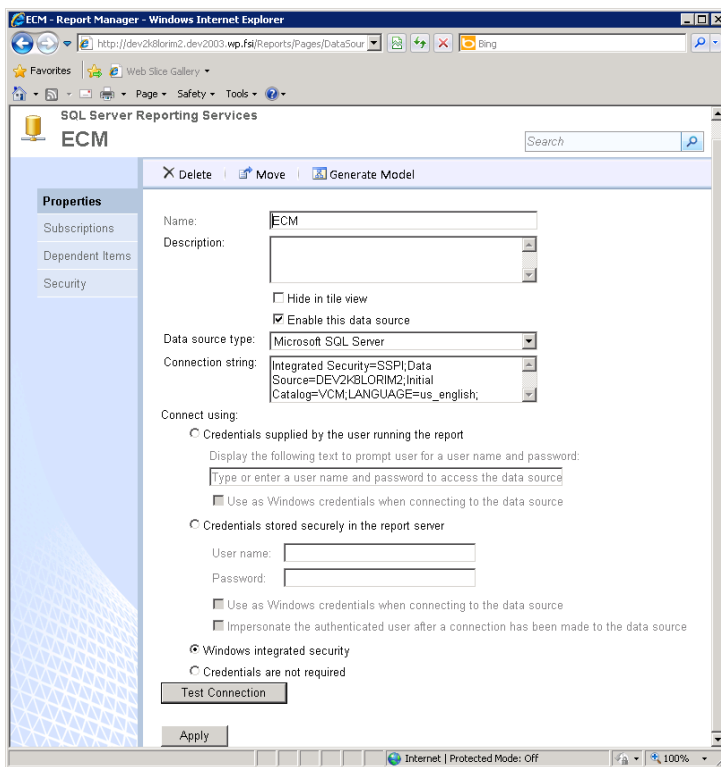
5. Click **Execute**.
6. Right-click the **SQL Server Reporting Services (MSSQLSERVER)** service and select **Start**.
7. Open a command window and reset the encrypted key store using the command `rskeymgmt -d`, and when prompted to delete all encrypted data from the report server database, enter `y`.
8. Enter `rsconfig -c -s <SQLSERVERNAME> -d ReportServer -a Windows`, and wait for the command to complete successfully.
9. Restart the SQL Server Reporting Services service.
10. Restart IIS using the command `iisreset /restart`, and wait for the IIS services to stop and restart successfully.
11. Open Internet Explorer and enter `http://[SERVERNAME]/Reports/` to navigate to the Report Server and verify that SSRS is operating properly.



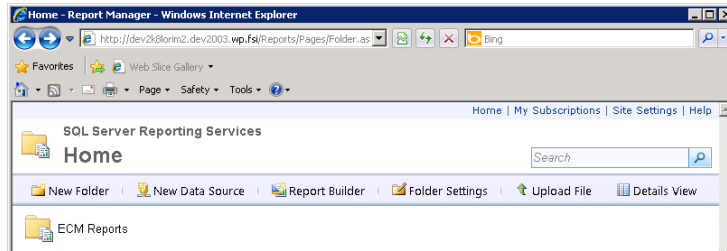
12. In the Report Manager window, select **ECM Reports** to access and edit the shared connection string.



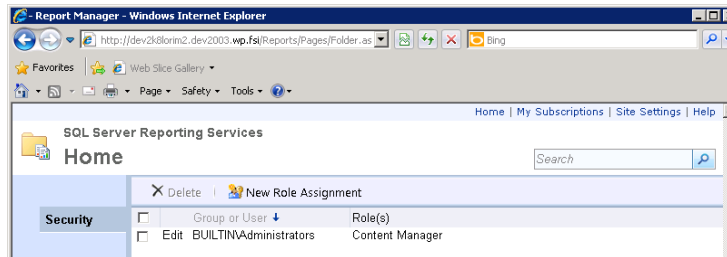
13. Click **ECM** to select the shared data source. The Properties General tab appears, displaying the Connection string.



14. Select **Windows integrated Security** and enter the value into the **Connection string** field:
`Integrated Security=SSPI;Data Source=SERVERNAME;Initial Catalog=VCM;LANGUAGE=us_english;`
15. Click **Test Connection** to ensure the connection is created successfully, and click **Apply**.
16. Click **Home** to return to the SSRS home page.



- Click **Folder Settings** to begin the process of removing any stranded accounts in SSRS.



- If any users other than the BUILTIN\Administrators and ECMSRSUser exist, click the check box next to each user account and click **Delete**.

Restore the VCM Databases

You must restore the VCM Databases.

Procedure

- Log into SQL Server Management Studio as a user with Administrative privileges.
- Enter this command to restore the VCM database and click **Execute**:

```
RESTORE DATABASE [VCM]
FROM DISK = N'E:\Backup\VCM\VCM_backup_201003021337.bak'
WITH FILE=1, NOUNLOAD, REPLACE, STATS = 10
GO
```

- Enter this command to restore the VCM_UNIX database and click **Execute**:

```
RESTORE DATABASE [VCM_UNIX]
FROM DISK = N'E:\Backup\VCM_UNIX\VCM_UNIX_backup_201003021337.bak'
WITH FILE=1, NOUNLOAD, REPLACE, STATS = 10
GO
```

- Enter this command to restore the VCM_Coll database and click **Execute**:

```
RESTORE DATABASE [VCM_Coll]
FROM DISK = N'E:\Backup\VCM_Coll\VCM_Coll_backup_201003021337.bak'
WITH FILE=1, NOUNLOAD, REPLACE, STATS = 10
GO
```

- Enter this command to restore the CSI_Domain database and click **Execute**:

```
RESTORE DATABASE [CSI_Domain]
FROM DISK = N'E:\Backup\CSI_Domain\CSI_Domain_backup_201003021337.bak'
WITH FILE=1, NOUNLOAD, REPLACE, STATS = 10
GO
```

6. Drop the definition of the VCM_Raw database, which is a temporary database that is automatically re-created during the installation.

```
IF EXISTS (SELECT name FROM sys.databases WHERE name = N'VCM_Raw')
DROP DATABASE [VCM_Raw]
```

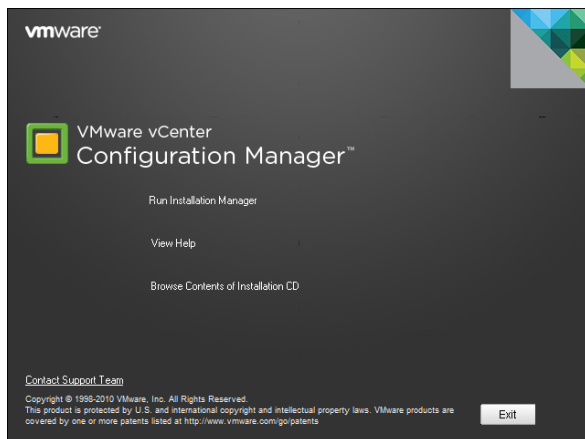
7. Update the path of exported reports using ["Script for Exported Reports" on page 43](#).

Installing VCM

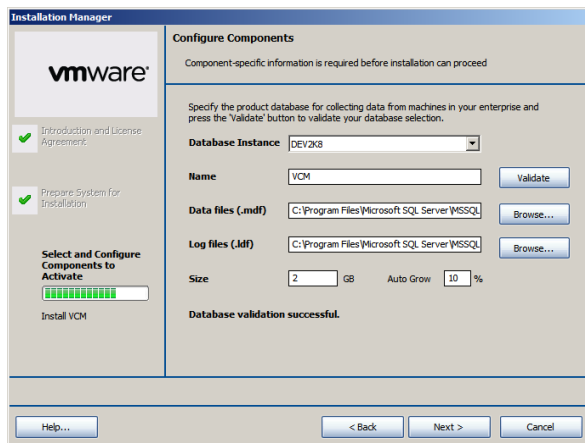
The recovery server is now ready for you to install VCM. During the installation, select the existing database instances and certificates. For all other installation options, see the VCM Installation Manager online Help.

Procedure

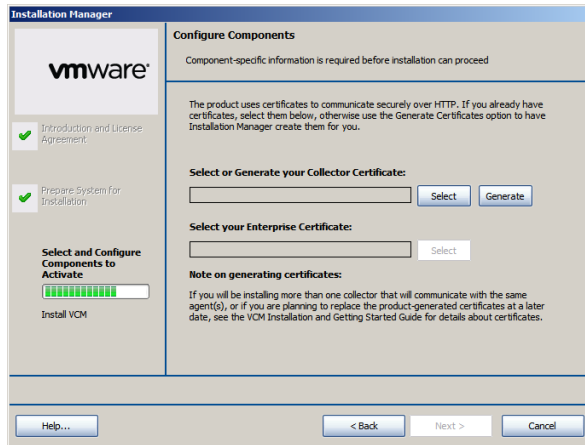
1. Start the VCM installation.



2. Select Run Installation Wizard and continue through the wizard to the Configure Components page that shows the **Database Instance**.



3. When prompted to select a database instance, make sure your existing database name is selected and click **Validate**.
4. Continue through the wizard to the page to select or generate certificates.



5. When prompted to select or generate a certificate for HTTP Agents, click **Select**, and then select the **VMware VCM Collector Certificate** to use the existing HTTP Certificate. The Collector Certificate and Enterprise Certificate fields will populate with the selected certificate.
6. Continue through the installation until the process completes and click **Finish** to complete the installation.

Restoring File System Components

After the VCM installation completes, restore the file system components from the `CMFiles$` share locations, along with any other corporate standard items. If additional custom components are installed, refer to the disaster recovery guides for each customization.

Script for Exported Reports

The majority of scheduled reports exported from the old Collector include a hard-coded server name. The scripts update the old server name export location with the new name by modifying the parameters passed and the UI string.

Any UI strings that are greater than 8000 characters must be handled differently. In these cases, the exports will work properly. However, if you edit the scheduled job the report shows the old location.

If you edit one of these exceptions and click **Finish** without first correcting the export location, the connection to the report will break.

IMPORTANT Before you run this script, edit the `@oldserver` and `@newserver` variables.

```
Declare @oldserver varchar(32)
Declare @newserver varchar(32)

set @oldserver = 'OLDSERVERNAME'
set @newserver = 'NEWSERVERNAME'

update dbo.ecm_rpt_reports_scheduled
set export_path = '\\\' +
    @newserver +
    substring(export_path, len(@oldserver)+3, len(export_path) -
    (len(@oldserver)+2))
where export_path like '%\' + @oldserver + '%\'

update dbo.ecm_sysdat_actions_ui_definition_text_xref
set definition_text =
    replace(cast(definition_text as varchar(max)), @oldserver, @newserver)
where
    definition_text like '%\' + @oldserver + '%\'
```


Index

A			
about this book	5		
accessibility to SRS report folder	29		
B			
back up additional files			
customizations to Collector	23		
reports exported	23		
backup procedures	9		
database	9		
differential, daily	17		
file system	23		
full backup	10		
HTTP Certificates	23		
C			
certificates	23		
import	30		
compliance	9		
corporate standards	9		
D			
daily/differential backup	17		
database			
backup	9		
restoration	35, 37		
disaster recovery plan	7		
duplicate hardware	7		
F			
file system			
backup	23		
restoration	43		
full backup	10		
H			
historical data	7		
HTTP certificates	23		
import	30		
I			
import HTTP certificates	30		
installation	41		
M			
maintenance plan	9		
R			
recovery			
Collector	7		
procedures	29		
server installation	41		
report folder access	29		
		restore databases	35
		configuration management	39
		report server	37
		system	35
		restore file system components	43
		S	
		SRS report folder	29

