



Backup and Recovery Guide

Product Information

This document applies to IBM Cognos Series 7 Deployment Manager Version 5 and may also apply to subsequent releases. To check for newer versions of this document, visit the IBM Cognos Information Centers (<http://publib.boulder.ibm.com/infocenter/cogic/v1r0m0/index.jsp>).

Copyright

Licensed Materials - Property of IBM

© Copyright IBM Corp. 2000, 2010.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

IBM, the IBM logo, ibm.com, and Cognos are trademarks or registered trademarks of International Business Machines Corp., in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at www.ibm.com/legal/copytrade.shtml.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both. UNIX is a registered trademark of The Open Group in the United States and other countries.

Table of Contents

Introduction	5
Chapter 1: Back Up and Restore Series 7 Applications	7
Backing Up and Restoring in Windows	7
Back Up and Restore Configuration Settings in Windows	7
Back Up and Restore Access Manager Information in Windows	8
Back Up and Restore the Directory Server Data in Windows	9
Back Up and Restore Upfront in Windows	10
Back Up and Restore PowerPlay Enterprise Server Metadata in Windows	11
Back Up and Restore Impromptu Web Reports Data in Windows	12
Back Up and Restore IBM Cognos NoticeCast in Windows	15
Back Up and Restore IBM Cognos Visualizer in Windows	15
Backing Up and Restoring in UNIX	16
Back Up and Restore Configuration Settings in UNIX	16
Back Up and Restore Access Manager Information in UNIX	17
Back Up and Restore the Directory Server Data in UNIX	17
Back Up and Restore Upfront in UNIX	18
Back Up and Restore PowerPlay Enterprise Server Metadata in UNIX	19
Back Up and Restore Impromptu Web Reports Data in UNIX	20
Back Up and Restore IBM Cognos NoticeCast in UNIX	23
Back Up and Restore IBM Cognos Visualizer in UNIX	23
Index	25

Introduction

Note: Some Asian languages are not supported by IBM Cognos Impromptu, IBM Cognos Impromptu Web Reports, and IBM Cognos Visualizer.

Finding information

To find the most current product documentation, including all translated documentation, access one of the IBM Cognos Information Centers at <http://publib.boulder.ibm.com/infocenter/cogic/v1r0m0/index.jsp>.

You can also read PDF versions of the product release notes and installation guides directly from IBM Cognos product disks.

Samples disclaimer

The Great Outdoors Company, GO Sales, any variation of the Great Outdoors name, and Planning Sample depict fictitious business operations with sample data used to develop sample applications for IBM and IBM customers. These fictitious records include sample data for sales transactions, product distribution, finance, and human resources. Any resemblance to actual names, addresses, contact numbers, or transaction values, is coincidental. Other sample files may contain fictional data manually or machine generated, factual data compiled from academic or public sources, or data used with permission of the copyright holder, for use as sample data to develop sample applications. Product names referenced may be the trademarks of their respective owners. Unauthorized duplication is prohibited.

Chapter 1: Back Up and Restore Series 7 Applications

This document describes how to back up and restore Series 7 applications in Windows and UNIX environments.

Assumptions

The procedures provided here assume the following:

- That for multiple-server installations, you must repeat some of the steps on each server.
- You installed IBM Cognos Series 7 products in the default location, C:\Program Files\Cognos\cern in Windows, and /usr/cognos/cern in UNIX, where *n* is the rendition number of the version you installed, such as cer5 or cer6.
- You will not change the directory locations when you restore IBM Cognos products.

If you plan to move the application, use these procedures to back up the application, and then use IBM Cognos Deployment Manager to move the application.

- You are using Bourne shell commands for UNIX.
- You have administrative privileges to perform backup and restore procedures.
- You will create a backup directory before you start the backup procedure.

Backing Up and Restoring in Windows

Backing up and restoring is the process of saving IBM Cognos configuration files and data files to one location so that you can incorporate them into your backup strategy.

Some IBM Cognos products and components have services that must be stopped before you begin the backup process. These services must be started when you complete the restore process.

Tip: You can use Configuration Manager to stop and start your product and component services. You can also stop and start services using the Control Panel.

Back Up and Restore Configuration Settings in Windows

If you changed the property values of your IBM Cognos products or components, you must save the customized configurations as a Configuration Specification file (.ccs) if you want to reuse them. You can then reapply the configuration file when needed.

Use Configuration Manager to back up and restore Series 7 configurations.

Steps to Back Up

1. Start Configuration Manager.

2. Click **Open the current configuration**.
3. From the **File** menu, click **Save As**.
4. In the **File name** box, type a name for the Configuration Specification file (.ccs).
5. In the **Save in** box, select the location to save your file, and click **Save**.

Steps to Restore

1. Start Configuration Manager.
2. From the **File** menu, click **Open a configuration from a file**.
3. Browse for the file, and click **Open**.
Confirm that the configuration settings are correct.
4. In the **Explorer** pane, click the computer name.
5. From the **Actions** menu, click **Apply Selection**.
A message states that this action will apply configurations to the computer you are working on.
6. Click **Yes**.
7. From the **Actions** menu, click **Start Service**.
A message states that this action will start components to the computer you are working on.
8. Click **Yes**.
The services are registered and started.

Back Up and Restore Access Manager Information in Windows

Access Manager provides a centralized environment to define, store, and maintain security information for IBM Cognos business information applications.

You store authentication data in one of the following sources:

- a namespace on an LDAP directory server
- a local authentication export file (.lae)

If you want to maintain your security information, you must back up and restore the authentication information by exporting it. You can use Access Manager-Administration to back up and restore Series 7 security.

Alternatively, you can back up your entire directory server database. For more information, see "Back Up and Restore the Directory Server Data on Windows".

Steps to Back Up

1. Start Access Manager - Administration.
2. In the **Authentication Information** pane, click the namespace that you want to back up.

3. From the **Action** menu, click **Log On**, and type your logon information.
4. Click the namespace.
5. From the **Action** menu, click **Export to .LAE File**.
6. Click **Add**.
7. Type a **Logical name** and enter a **File name** for the local authentication export file (.lae), then click **OK**.
8. Click **Empty the target namespace**.
9. Click **Export**.

Steps to Restore

1. Start Access Manager - Administration.
2. In the **Authentication Information** pane, click the namespace that you want to restore.
3. From the **Action** menu, click **Log On**, and type your logon information.
4. Click the namespace.
5. From the **Action** menu, click **Import from .LAE File**.
6. Click the correct local authentication export file (.lae), and then click the namespace.
7. Click **Empty the target namespace**.
8. Click **Import**.

Back Up and Restore the Directory Server Data in Windows

If you are using a directory server to store Access Manager security information, you can back up and restore the entire directory server database using an LDAP Data Interchange Format (.ldif) file. The .ldif file contains information about the directory server database, as well as information specific to Access Manager, such as namespaces.

The following information indicates how to backup the data for a SunONE directory server.

Use the directory server console to import and export the directory server data into an .ldif file, then use the .ldif to restore the information into a directory server.

For more information, see the Sun Web site or your third-party documentation.

Steps to Backup

1. Open your directory server console and log on.
For a list of supported versions, see your directory server documentation.
2. In the **Console** window, expand the **server host**, and the **Server Group** folder, and then double-click on the directory server used by your IBM Cognos Series 7 products.
3. Click the **Configuration** tab.

4. From the **Console** menu, click **Export**.
5. In the **Export Database** dialog, specify a secure location and filename for the .ldif, then click **OK**.

Steps to Restore

1. Open your directory server console and log on.
2. In the **Servers and Applications** window, expand the **server host**, and the **Server Group** folder, then double-click on the new directory server to be used by your IBM Cognos Series 7 products.
3. Click the **Configuration** tab.
4. From the **Console** menu, click **Initialize Databases**.
5. Enter the name of the .ldif you created earlier.
6. In the **Initialize Database** column, ensure the check box is selected, and then click **OK**.

A message appears, warning that the operation will overwrite certain information and certain conditions may affect the success of the initialization.

7. Click **Yes**.

Back Up and Restore Upfront in Windows

Upfront is the customizable user interface that you use to view, find, organize and share IBM Cognos reports and queries on the Web. You back up and restore the Upfront data store to preserve all the information about the resources that Upfront manages, in case any of the information is lost or corrupted.

To either backup or restore the data store, you must run the upfdbadm.exe utility on the computer where the data store is installed.

IBM Cognos does not support a "hot" restore of the Upfront data store. This means that before you restore the data store, you must stop the Upfront dispatcher. If a hot restore of the Upfront data store is performed, errors may occur.

When you back up Upfront, you must back up your security information, and the data stores for the IBM Cognos products referenced by NewsItems in this NewsIndex. For more information, see "Back Up and Restore Access Manager Information in Windows".

If you change your administrator password and restore the data store at a later time, the data store password and the administrator password will not be synchronized. When you start Upfront after restoring the data store, Upfront displays an error message indicating that Upfront could not log in to the database server. To resolve this problem, change the data store password. For information, see the section on administering the data store in the *Upfront Server Administration Guide*.

In the following steps, specific version numbers for a release are substituted for an italicized letter *n* (*n*). For example, the *cer n* folder substitutes the rendition number of your IBM Cognos files. The rendition number depends on the version you installed, such as cer5 or cer6.

When you restore the Upfront data store you must also restore your security information and the data store for all the IBM Cognos products referenced by NewsItems in this NewsIndex.

Steps to Back Up

1. Start Upfront.
Ensure that the data store is started.
2. Open the **Command Prompt** window.
3. Run upfdbadm.exe with the -b parameter, and type the location and name of the backup file.
For example, type the following:

```
c:\Program Files\Cognos\cern\bin\upfdbadm.exe
-b c:\backup\UpfrontStore.bak
```
4. Close the **Command Prompt** window.

Steps to Restore

1. Start Upfront.
Ensure that the data store is started.
2. Open the **Command Prompt** window.
3. Run upfdbadm.exe with the -r parameter, and type the location and name of the backup file.
This will restart the Upfront server and disconnect all active users.
For example, type the following:

```
c:\Program Files\Cognos\cern\bin\upfdbadm.exe
-r c:\backup\UpfrontStore.bak
```
4. Close the **Command Prompt** window.

Back Up and Restore PowerPlay Enterprise Server Metadata in Windows

When using PowerPlay Enterprise Server, you create a set of directories and files that represent your PowerPlay Enterprise Server metadata. To protect your PowerPlay Enterprise Server metadata from corruption, you may want to keep backup copies of this information.

If you use Access Manager and Upfront as part of PowerPlay Enterprise Server, you must also back up their metadata. For more information about these topics, see "Back Up and Restore Access Manager Information in Windows", or "Back Up and Restore Upfront in Windows".

In the following steps specific version numbers for a release are substituted for an italicized letter *n* (*n*). For example, the *cern* folder substitutes the rendition number of your IBM Cognos files. The rendition number depends on the version you installed, such as cer5 or cer6.

Steps to Back Up

1. Stop the services for PowerPlay Enterprise Server (*cern*), on all of the computers in the server group.
2. Open Windows Explorer.

3. Go to the Cognos\cern\ppserver directory.
4. Copy the PPSRoot.cfx file to the backup location.
5. Copy the PPSRoot directory, its contents, and all subfolders, to the backup location.

If you are using the **Mount At** property to store or share metadata across multiple servers, you must locate that data using the PowerPlay Server Administration tool and copy it to the backup location.

6. Copy any required cubes (.mdc), or report files (.ppx) to the backup location.

Tip: To locate your cube files or your report files, use the PowerPlay Server Administration tool and check the **Cube Source** property.

7. If you use audit information, copy audit files to a backup location.

Audit files are named ppes_audit.log and are located in ppserver directory. For more information about audit files, see the *PowerPlay Enterprise Server Guide*.

Steps to Restore

1. Stop the services for PowerPlay Enterprise Server (cern), on all of the computers in the server group.
2. Go to the Cognos\cern\ppserver directory.
3. Delete the PPSRoot.cfx file.
4. Delete the PPSRoot directory, its contents, and all subfolders.
5. Copy the PPSRoot.cfx backup file to Cognos\cern\ppserver.
6. Copy the backed-up PPSRoot directory, its contents and all subfolders, to Cognos\cern\ppserver.
7. Copy the backed-up cubes (.mdc) and reports (.ppx) to the correct folder location.
8. Copy the **Mount At** directories to the original folder location.
9. Copy audit files to the ppserver directory.
10. Start the services for PowerPlay Enterprise Server (cern), on all of the computers in the server group.

Back Up and Restore Impromptu Web Reports Data in Windows

When using Impromptu Web Reports, you can create files that represent your Impromptu Web Reports data. To protect your Impromptu Web Reports data from corruption, accidental loss, or destruction, you can keep backup copies of this information.

Use iwrcmmand, osbackup, and osrestore to back up and restore Impromptu Web Reports. When you back up Impromptu Web Reports, you must also back up Access Manager and Upfront. For more information about these topics, see "Back Up and Restore Access Manager Information in Windows", or "Back Up and Restore Upfront in Windows". For more information on iwrcmmand, see the *IWR Command Developer Guide*.

The recommended method for automating Impromptu Web Reports backups is to use `iwrcommand` to disable the Impromptu Web Reports servers while the Impromptu Web Reports service continues to run on each server. Then use `osbackup` to back up the database (.db) files. This approach gives you more control over the backup procedure, especially in a multiple server configuration, and allows you to minimize any potential disruption in service as a result.

Alternatively, you can stop the Impromptu Web Reports services on all servers before using `osbackup` to back up the database files. In this case, be sure to wait for any running reports to complete before proceeding with the backup.

In the following steps specific version numbers for a release are substituted for an italicized letter *n* (*n*). For example, the *cern* folder substitutes the rendition number of your IBM Cognos files. The rendition number depends on the version you installed, such as *cer5* or *cer6*.

Either from the command prompt, or from a script, perform the following steps.

Steps to Back Up

1. Use the `iwrcommand EnableDisableServer` command to disable the Impromptu Web Reports servers.

Note: This command has options that allow you to choose the action to take if reports are executing at the time the command is run. For more information, see the *IWRCommand Developer Guide*.

For example, create a text file named `disableiwr.xml` that contains the command to disable all Impromptu Web Reports servers and stop and requeue any currently running reports:

```
<iwr:EnableDisableServer>
    <iwr:ServerName>ALL</iwr:ServerName>
    < iwr:Action>DISABLE</ iwr:Action>
    < iwr:Jobs>REQUEUE</ iwr:Jobs>
    < iwr:Timeout>300</ iwr:Timeout>
</iwr:EnableDisableServer>
```

Use `disableiwr.xml` as input to `iwrcommand`:

```
iwrcommand -f disableiwr.xml -g http://<server>/cognos/cgi-bin/imrap.cgi -u
administrator -p ""
```

2. Use `osbackup` to back up the Impromptu Web Reports databases.

Create a text file named `import_list.txt` that lists the fully qualified names of the Impromptu Web Reports database files to be backed up, in the following format:

`\Program Files\Cognos\cern\iwr\database\filename`

For example, create a file named `import_list.txt` that contains the following lines:

```
C:\Program Files\Cognos\cern\iwr\database\iwr7
4.db
C:\Program Files\Cognos\cern\iwr\database\iwr74job.db
C:\Program Files\Cognos\cern\iwr\database\iwr74Msg.db
C:\Program Files\Cognos\cern\iwr\database\iwr74SM.db
```

Create the backup directory, for example `C:\Backup`, before you run the `osbackup` command.

Run `osbackup` with the `-f`, `-i`, and `-I` parameters, using the `import_list.txt` file you created as input. For example, type the following, where *inc.lst* is a unique file name and *location* represents the absolute path where you created the `import_list.txt` file:

```
C:\ODI\Ostore\bin\osbackup -f C:\Backup\IWRDbBackup.bak
-i C:\backup\inc.lst -I location\import_list.txt
```

The `.bak` file is always created, even if there is an error. You must delete this file before running the command again.

3. Copy all report store files (including subdirectories and their contents) to a backup location, using any file copy command or utility.

Note: You can use `iwrconfig` with the `dumpAllReportSet` command to get a list of all report set locations. For example, type the following, where *filename* is the name of the file to which the report set information will be written:

```
C:\Program Files\Cognos\cern\bin\iwrconfig
-cmd dumpAllReportSet >>filename
```

You should also copy the file containing the current list of report set locations to the backup location.

4. Copy all audit files to a backup location, using any file copy command or utility.

The default location for these files is `C:\Program Files\Cognos\cern\logs\audit`. Check that this location has not been changed in Configuration Manager. For more information, see the Configuration Manager *User Guide*.

5. Use the `iwrcommand EnableDisableServer` command to enable the Impromptu Web Reports servers.

For example, create a text file named `enableiwr.xml` that contains the command to enable all Impromptu Web Reports servers:

```
<iwr:EnableDisableServer>
  <iwr:ServerName>ALL</iwr:ServerName>
  < iwr:Action>ENABLE</ iwr:Action>
</iwr:EnableDisableServer>
```

Use `enableiwr.xml` as input to `iwrcommand`:

```
iwrcommand -f enableiwr.xml -g http://<server>/cognos/cgi-bin/imrap.cgi
-u administrator -p ""
```

Steps to Restore

1. Stop the services for Impromptu Web Reports.
2. Delete all database files (`.db`) in the IWR database folder.

For example, this location may be:

```
\Program Files\Cognos\cern\iwr\database\*.db
```

3. Open the **Command Prompt** window.
4. Run `osrestore` with the `-a`, `-0`, and `-f` parameters.

For example,

```
C:\ODI\Ostore\bin\osrestore -a -0 -f
```

```
C:\backup\IWRDbBackup.bak
```

5. Close the **Command Prompt** window.
6. Copy the backed-up report sets to the correct directories. The files are located in the *filename* directory.
7. Copy the backed-up audit files to the audit file location. By default, this location is C:\Program Files\Cognos\cern\logs\audit.
8. Start the services for Impromptu Web Reports.

Back Up and Restore IBM Cognos NoticeCast in Windows

The IBM Cognos NoticeCast data store resides in a third-party DB2, Informix, Oracle, or SQL server database. Use your database administration tools to back up and restore the IBM Cognos NoticeCast data store. When you back up IBM Cognos NoticeCast, you must also back up Upfront and Access Manager. For more information about these topics, see "Back Up and Restore Access Manager Information in Windows", or "Back Up and Restore Upfront in Windows".

Back Up and Restore IBM Cognos Visualizer in Windows

You can create backup copies of your IBM Cognos Visualizer configuration data, visualizations, and data sources. If your data becomes corrupt, you can restore the backup files you created.

In the following steps specific version numbers for a release are substituted for an italicized letter *n* (*n*). For example, the *cern* folder substitutes the rendition number of your IBM Cognos files. The rendition number depends on the version you installed, such as *cer5* or *cer6*.

Steps to Back Up

1. Stop the services for IBM Cognos Visualizer Web Server.
2. Open Windows Explorer.
3. Go to Cognos\cern\bin
4. Copy the VizWebConfig.dat file to the backup location.
5. Copy any required visualization files (.viz) that are installed on the server to the backup location.

Tip: You can locate your visualizations using the IBM Cognos Visualizer Web Server Administration tool. Highlight the visualization. From the **File** menu click **Properties**, and then **Visualization**. Click the **Source** tab.
6. Copy any required data sources, including cubes (.mdc), Impromptu query definition files (.iqd), Excel spreadsheet files (.xls), and comma separated value files (.csv) to the backup location.

Tip: You can use IBM Cognos Visualizer to locate the data sources used in your visualizations. Open a visualization. From the **File** menu, click **Properties**, and then click the **Data Source** tab. To view the path for a data source, click the name of the data source and then click **Properties**.

Note: If you are using a relational database such as Oracle or Sybase as a data source, you must follow the steps in the administration guide for the relational database to back up the database.

7. Start the services for IBM Cognos Visualizer Web Server.

Steps to Restore

1. Stop the services for IBM Cognos Visualizer Web Server.
2. Go to `Cognos\cern\bin`
3. Delete the `VizWebConfig.dat` file.
4. Copy the `VizWebConfig.dat` backup file to `Cognos\cern\bin`
5. Copy the visualization files (`.viz`) you backed up to the correct folder location.
6. Copy the data sources you backed up to the correct locations.

Note: If you are using a relational database such as Oracle or Sybase as a data source, you must follow the steps in the administration guide for the relational database to restore the database.

7. Start the services for IBM Cognos Visualizer Web Server.

Backing Up and Restoring in UNIX

Backing up and restoring is the process of saving IBM Cognos configuration files and data files to one location so that you can incorporate them into your backup strategy.

The UNIX commands used in this document are for Bourne shell.

Back Up and Restore Configuration Settings in UNIX

If you changed the property values of your IBM Cognos products or components, you must save the customized configurations as a file if you want to reuse them. You can then reapply the configuration file when needed.

Use Configuration Manager to back up and restore Series 7 configurations.

In the following steps specific version numbers for a release are substituted for an italicized letter *n* (*n*). For example, the `cern` folder substitutes the rendition number of your IBM Cognos files. The rendition number depends on the version you installed, such as `cer5` or `cer6`.

Steps to Back Up

1. Go to `/usr/cognos/cern/bin`.
2. Type `configure`.
3. Type `opencurrent`.

A configuration specification file (`.ccs`) is created based on the computer you are working on.

4. Type the following, where `location/filename.ccs` is a directory and file name to which you have write access:

save *location/filename.ccs*

5. Type **exit**.

Steps to Restore

1. Go to `/usr/cognos/cern/bin`
2. Type **configure**.
3. Type the following, where *location/filename.ccs* is the configuration that you want to restore:
`openfile location/filename.ccs`
4. Type **apply**.
5. Type **start** to start the processes.
6. Type **exit**.

Back Up and Restore Access Manager Information in UNIX

Security information for Access Manager can be backed up and restored on a Windows computer that is communicating with a UNIX directory server. For more information, see "Back Up and Restore Access Manager Information in Windows".

Alternatively, you can back up your entire directory server database. For information about using an .ldif to backup and restore the directory server, see "Back Up and Restore the Directory Server in UNIX".

Back Up and Restore the Directory Server Data in UNIX

If you are using a directory server to store Access Manager security information, you can back up, and restore, the entire directory server database using an LDAP Data Interchange Format (.ldif) file. The .ldif file contains information about the directory server database, as well as information specific to Access Manager, such as namespaces. Use the directory server console to export, the directory server data into an .ldif file, then import the .ldif to restore the information into a directory server.

The following steps indicate how to backup the data for a SunONE directory server.

For more information, see the Sun Web site or your third-party documentation.

Steps to Back Up

1. Go to the `installation_location/usr/directory_server/servers`, and type
`./startconsole`
2. Log on to the directory server.
For a list of supported versions, see your directory server documentation.
3. In the **Console** window, expand the **server host**, and the **Server Group** folder, and then double-click on the directory server used by your existing IBM Cognos Series 7 products.

4. Click the **Configuration** tab.
5. From the **Console** menu, click **Export**.
6. In the **Export Database** dialog, specify a secure location, and the filename for the .ldif, then click **OK**.

Steps to Restore

1. Go to the *installation_location/ust/directory_server/servers*, and type `./startconsole`
2. Log on to the directory server Console.
SunONE suggests logging in as Directory Manager (for example, "**cn=Directory Manager**" with default password **admin1234**).
3. In the **Servers and Applications** window, expand the **server host**, then the **Server Group** folder, and then double-click on the new directory server to be used by the new version of IBM Cognos Series 7 products.
4. Click the **Configuration** tab.
5. From the **Console** menu, click **Initialize Databases**.
6. Enter the name of the .ldif you created earlier.
7. In the **Initialize Database** column, ensure the check box is selected, and then click **OK**.
A message appears, warning you that the operation will overwrite certain information, and that certain conditions may affect the success of the initialization.
8. Click **Yes**.

Back Up and Restore Upfront in UNIX

Upfront is the customizable user interface that you use to view, find, organize and share IBM Cognos reports and queries on the Web. You back up and restore the Upfront data store to preserve all the information about the resources that Upfront manages, in case any of the information is lost or corrupted.

To either backup or restore the data store, you must run the `upfdbadm.exe` utility on the computer where the data store is installed.

IBM Cognos does not support a "hot" restore of the Upfront data store. This means that before you restore the data store, you must stop the Upfront dispatcher. If a hot restore of the Upfront data store is performed, errors may occur.

When you back up Upfront, you must back up your security information, and the data stores for the IBM Cognos products referenced by NewsItems in this NewsIndex. For more information, see "Back Up and Restore Access Manager Information in Windows".

If you change your administrator password and restore the data store at a later time, the data store password and the administrator password will not be synchronized. When you start Upfront after

restoring the data store, Upfront displays an error message indicating that Upfront could not log in to the database server. To resolve this problem, change the data store password. For information, see the section on administering the data store in the *Upfront Server Administration Guide*.

In the following steps, specific version numbers for a release are substituted for an italicized letter *n* (*n*). For example, the *cern* folder substitutes the rendition number of your IBM Cognos files. The rendition number depends on the version you installed, such as *cer5* or *cer6*.

When you restore the Upfront data store you must also restore your security information, and the data store for all the IBM Cognos products referenced by NewsItems in this NewsIndex.

Steps to Back Up

1. Start the processes for Upfront.
Ensure that the data store is started.
2. Go to the `/usr/cognos/cern/bin` directory.
3. Run UpfDBAdm with the `-b` parameter.
For example, type

```
run-upfdbadm -b ./UpfDatastore.bak
```

Steps to Restore

1. Start the processes for Upfront.
Ensure that the data store is started.
2. Go to the `/usr/cognos/cern/bin` directory.
3. Run UpfDBAdmdm with the `-r` parameter.
For example, type

```
run-upfdbadm -r ./UpfDatastore.bak
```
4. Go to the `/usr/cognos/cern/bin` directory.
5. Restart the Upfront processes.

When you restore the Upfront data store you must also restore your security information, and the data store for all the IBM Cognos products referenced by NewsItems in this NewsIndex.

Back Up and Restore PowerPlay Enterprise Server Metadata in UNIX

When using PowerPlay Enterprise Server, you will create a set of directories and files that represent your PowerPlay Enterprise Server metadata. To protect your PowerPlay Enterprise Server metadata from corruption, you may want to keep backup copies of this information.

If you use Access Manager and Upfront as part of PowerPlay Enterprise Server, then you must also back up their metadata. For more information about these topics, see "Back Up and Restore Access Manager Information in UNIX", or "Back Up and Restore Upfront in UNIX".

In the following steps specific version numbers for a release are substituted for an italicized letter *n* (*n*). For example, the *cern* folder substitutes the rendition number of your IBM Cognos files. The rendition number depends on the version you installed, such as *cer5* or *cer6*.

Steps to Back Up

1. Stop the processes for PowerPlay Enterprise Server.
2. Go to the `/usr/cognos/cern/ppserver` directory.
3. Copy the `PPSRoot.cfx` file to the backup location.
4. Copy the `PPSRoot` directory and its contents to the backup location.

If you are using the **Mount At** property to store or share metadata across multiple servers you must locate that data using the PowerPlay Server Administration tool and copy it to the backup location.

5. Copy any required cubes (`.mdc`), or report files (`.ppx`) to the backup location.

Tip: To locate your cube files or your report files, use the PowerPlay Server Administration tool and check the **Cube Source** property.

Steps to Restore

1. Stop the processes for PowerPlay Enterprise Server.
2. Go to the `/usr/cognos/cern/ppserver` directory.
3. Delete the `PPSRoot.cfx` file.
4. Delete the `PPSRoot` directory and its contents.
5. Copy the `PPSRoot.cfx` backup file to `/usr/cognos/cern/ppserver`.
6. Copy the backed-up `PPSRoot` directory and its contents to `/usr/cognos/cern/ppserver`.
7. Copy the backed-up cubes (`.mdc`) and reports (`.ppx`) to the correct folder location.
8. Copy the **Mount At** directories to the original folder location.
9. Start the processes for PowerPlay Enterprise Server.

Back Up and Restore Impromptu Web Reports Data in UNIX

When using Impromptu Web Reports, you can create files that represent your Impromptu Web Reports data. To protect your Impromptu Web Reports data from corruption, accidental loss, or destruction, you can keep backup copies of this information.

Use `iwrcommand`, `osbackup`, and `osrestore` to back up and restore Impromptu Web Reports. When you back up Impromptu Web Reports, you must also back up Access Manager and Upfront. For more information about these topics, see "Back Up and Restore Access Manager Information in UNIX", or "Back Up and Restore Upfront in UNIX". For more information on `iwrcommand`, see the *IWR Command Developer Guide*.

The recommended method for automating Impromptu Web Reports backups is to use `iwrcommand` to disable the Impromptu Web Reports servers while the Impromptu Web Reports service continues to run on each server. Then use `osbackup` to back up the database (.db) files. This approach gives you more control over the backup procedure, especially in a multiple server configuration, and allows you to minimize any potential disruption in service as a result.

Alternatively, you can stop the Impromptu Web Reports processes on all servers before using `osbackup` to back up the database files. In this case, be sure to wait for any running reports to complete before proceeding with the backup.

In the following steps specific version numbers for a release are substituted for an italicized letter *n* (*n*). For example, the *cern* folder substitutes the rendition number of your IBM Cognos files. The rendition number depends on the version you installed, such as *cer5* or *cer6*.

Either from the command prompt, or from a script, perform the following steps.

Steps to Back Up

1. Use the `iwrcommand EnableDisableServer` command to disable the Impromptu Web Reports servers.

Note: This command has options that allow you to choose the action to take if reports are executing at the time the command is run. For more information, see the *IWRCommand Developer Guide*.

For example, create a text file named `disableiwr.xml` that contains the command to disable all Impromptu Web Reports servers and stop and requeue any currently running reports:

```
<iwr:EnableDisableServer>
  <iwr:ServerName>ALL</iwr:ServerName>
  < iwr:Action>DISABLE</ iwr:Action>
  < iwr:Jobs>REQUEUE</ iwr:Jobs>
  < iwr:Timeout>300</ iwr:Timeout>
</iwr:EnableDisableServer>
```

Use `disableiwr.xml` as input to `iwrcommand`:

```
iwrcommand -f disableiwr.xml -g http://<server>/cognos/cgi-bin/imrap.cgi -u
administrator -p ""
```

2. Use `osbackup` to back up the Impromptu Web Reports databases.

Create a text file named `import_list.txt` that lists the fully qualified names of the Impromptu Web Reports database files to be backed up, in the following format:

```
/usr/cognos/cern/iwr/database/filename
```

For example, create a file named `import_list.txt` that contains the following lines:

```
/usr/cognos/cern/iwr/database/iwr74.db
/usr/cognos/cern/iwr/database/iwr74Job.db
/usr/cognos/cern/iwr/database/iwr74Msg.db
/usr/cognos/cern/iwr/database/iwr74SM.db
```

Create the backup directory, for example `C:\Backup`, before you run the `osbackup` command.

Run `osbackup` with the `-f`, `-i`, and `-I` parameters, using the `import_list.txt` file you created as input. For example, type the following, where *inc.lst* is a unique file name and *location* represents the absolute path where you created the `import_list.txt` file:

```
./osbackup -f /usr/backup/IWRDbBackup.bak -i /usr/backup/inc.lst -I
location/import_list.txt
```

The `.bak` file is always created, even if there is an error. You must delete this file before running the command again.

3. Copy all report store files (including subdirectories and their contents) to a backup location, using any file copy command or utility.

Note: You can use `iwrconfig` with the `dumpAllReportSet` command to get a list of all report set locations. For example, type the following, where *filename* is the name of the file to which the report set information will be written:

```
/usr/cognos/cern/bin/iwrconfig
-cmd dumpAllReportSet >> filename
```

You should also copy the file containing the current list of report set locations to the backup location.

4. Copy all audit files to a backup location, using any file copy command or utility.

The default location for these files is `/usr/cognos/cern/logs/audit`. Check that this location has not been changed in Configuration Manager. For more information, see the Configuration Manager *User Guide*.

5. Use the `iwrcommand EnableDisableServer` command to enable the Impromptu Web Reports servers.

For example, create a text file named `enableiwr.xml` that contains the command to enable all Impromptu Web Reports servers:

```
<iwr:EnableDisableServer>
  <iwr:ServerName>ALL</iwr:ServerName>
  < iwr:Action>ENABLE</ iwr:Action>
</iwr:EnableDisableServer>
```

Use `enableiwr.xml` as input to `iwrcommand`:

```
iwrcommand -f enableiwr.xml -g http://<server>/cognos/cgi-bin/imrap.cgi
-u administrator -p ""
```

Steps to Restore

1. Stop the processes for Impromptu Web Reports.
2. Delete all the database files (`.db`) in the database folder.

For example,

```
rm /usr/cognos/cern/iwr/database/*db
```

3. Go to the ObjectStore bin directory.

For example,

```
cd /opt/ODI/ostore/bin
```

4. Run `osrestore`.

For example, type

```
./osrestore -a -0 -f /usr/backup/IWRDbBackup.bak
```

5. Copy the backed-up report sets to the correct directories. The files are located in the *filename* directory.
6. Copy the backed-up audit files to the audit file location. By default, this location is `/usr/cognos/cern/logs/audit`.
7. Start the processes for Impromptu Web Reports.

Back Up and Restore IBM Cognos NoticeCast in UNIX

The IBM Cognos NoticeCast data store resides in a third-party DB2, Informix, Oracle, or SQL server database. Use your database administration tools to back up and restore the IBM Cognos NoticeCast data store. When you back up IBM Cognos NoticeCast, you must also back up Upfront and Access Manager. For more information about these topics, see "Back Up and Restore Access Manager Information in UNIX", or "Back Up and Restore Upfront in UNIX".

Back Up and Restore IBM Cognos Visualizer in UNIX

You can create backup copies of your IBM Cognos Visualizer configuration data, visualizations, and data sources. If your data becomes corrupt, you can restore the backup files you created.

In the following steps specific version numbers for a release are substituted for an italicized letter *n* (*n*). For example, the *cern* folder substitutes the rendition number of your IBM Cognos files. The rendition number depends on the version you installed, such as *cer5* or *cer6*.

Steps to Back Up

1. Stop the services for IBM Cognos Visualizer Web Server.
2. Go to `Cognos/cern/bin`
3. Copy the `VizWebConfig.dat` file to the backup location.
4. Copy any required visualization files (`.viz`) that are installed on the server to the backup location.

Tip: You can locate your visualizations using the IBM Cognos Visualizer Web Server Administration tool on your Windows computer. Highlight the visualization. From the **File** menu click **Properties**, and then **Visualization**. Click the **Source** tab.

5. Copy any required data sources, including cubes (`.mdc`), Impromptu query definition files (`.iqd`), Excel spreadsheet files (`.xls`), and comma separated value files (`.csv`) to the backup location.

Tip: You can use IBM Cognos Visualizer on your Windows computer to locate the data sources used in your visualizations. Open a visualization. From the **File** menu, click **Properties**, and then click the **Data Source** tab. To view the path for a data source, click the name of the data source and then click **Properties**.

Note: If you are using a relational database such as Oracle or Sybase as a data source, you must follow the steps in the administration guide for the relational database to back up the database.

6. Start the services for IBM Cognos Visualizer Web Server.

Steps to Restore

1. Stop the services for IBM Cognos Visualizer Web Server.
2. Go to `Cognos/cern/bin`
3. Delete the `VizWebConfig.dat` file.
4. Copy the `VizWebConfig.dat` backup file to `Cognos/cern/bin`.
5. Copy the visualization files (`.viz`) you backed up to the correct folder location.
6. Copy the data sources you backed up to the correct locations.

Note: If you are using a relational database such as Oracle or Sybase as a data source, you must follow the steps in the administration guide for the relational database to restore the database.

7. Start the services for IBM Cognos Visualizer Web Server.

Index

Symbols

.ccs files, 7, 16
.cfx files, 11, 19
.exe files, 10, 18
.ini files, 7, 12, 20
.ldif files, 17
.mdc files, 11, 19
.ppx files, 11, 19
.sh files, 18

A

Access Manager

back up and restore in UNIX, 17
back up and restore in Windows, 8

B

backing up and restoring

Access Manager in UNIX, 17
Access Manager in Windows, 8
cubes in UNIX, 19
cubes in Windows, 11
custom configurations in UNIX, 16
custom configurations in Windows, 7, 12
directory server in UNIX, 17
directory servers in Windows, 8
IBM Cognos NoticeCast in UNIX, 23
IBM Cognos NoticeCast in Windows, 15
IBM Cognos Visualizer in UNIX, 23
IBM Cognos Visualizer in Windows, 15
Impromptu Web Reports in UNIX, 20
Impromptu Web Reports in Windows, 12
in UNIX, 16
in Windows, 7
LDAP in UNIX, 17
namespaces in UNIX, 17
PowerPlay Enterprise Server in UNIX, 19
PowerPlay Enterprise Server in Windows, 11
security information in UNIX, 17
security information in Windows, 8
SunOne Directory Server in UNIX, 17

SunOne Directory Server in Windows, 9

Upfront in UNIX, 18

Upfront in Windows, 10

Bourne/Korn shell, 7

Bourne shell, 12

C

configuration files

back up and restore in UNIX, 16

back up and restore in Windows, 7

cubes

back up and restore in UNIX, 19

back up and restore in Windows, 11

customized configurations

back up and restore in UNIX, 16

back up and restore in Windows, 7, 12

D

directory servers

back up and restore in UNIX, 17

back up and restore in Windows, 8

I

IBM Cognos NoticeCast

back up and restore in UNIX, 23

back up and restore in Windows, 15

IBM Cognos Visualizer

back up and restore in UNIX, 23

back up and restore in Windows, 15

import_list.txt, 12

Impromptu Web Reports

back up and restore in UNIX, 20

back up and restore in Windows, 12

Introduction, 5

iwrconfig

back up and restore, 12

L

LAE files

back up and restore in UNIX, 17

back up and restore in Windows, 9

Index

LDAP

- back up and restore in UNIX, [17](#)
- back up and restore in Windows, [9](#)

LDAP data interchange file

- back up and restore in UNIX, [17](#)
- back up and restore in Windows, [9](#)

M

multiple-server installations

- back up and restore, [7](#), [12](#)

N

namespaces

- back up and restore in UNIX, [17](#)

O

osbackup, [12](#)

osrestore, [12](#)

P

PowerPlay Enterprise Server

- back up and restore in UNIX, [19](#)
- back up and restore in Windows, [11](#)

PPSRoot.cfx

- back up and restore in UNIX, [19](#)
- back up and restore in Windows, [11](#)

R

restoring

- back up Series 7 data, [7](#)

S

security information

- back up and restore in UNIX, [17](#)
- back up and restore in Windows, [8](#)

SunONE Directory Server

- back up and restore in UNIX, [17](#)
- back up and restore in Windows, [9](#)

U

UNIX

- back up and restore, [16](#)

upfdbadm.exe, [10](#), [18](#)

Upfront

- back up and restore in UNIX, [18](#)
- back up and restore in Windows, [10](#)