Business Objects™

BusinessObjects XI Release 2

Back up and Recovery Best Practices

Overview

The purpose of this document is to outline recommended steps to back up and recover data for key BusinessObjects XI Release 2 system components. These procedures are used to mitigate data loss, optimize data recovery, and minimize the delay before resumption of normal business operations.

Contents

Introduction

This document describes procedures for performing a back up of the Web and BusinessObjects Server system and data files, as well as the procedures to be followed to recover from data loss or hardware failure. The plan execution requires an experienced BusinessObjects Professional, OS System Administrator and Database Administrator.

When a BusinessObjects implementation is done on a staged system, the back up and recovery process is similar for all environments within the staged system; development, test, and production. Therefore, this document does not refer to any specific environment. It is recommended to back up all environments.

The document does not include recovery of a query data source and client tier. These components should be recovered according to existing business processes for databases and user workstations.

Back Up and Recovery Process Concept

A back up and recovery plan consists of precautions to be taken in the event of a full system failure due to a natural disaster or a catastrophic event. The plan aims to minimize the effects of the disaster on the daily operations so that the organization is able to maintain or quickly resume mission-critical functions. It is recommended, as part of a BusinessObjects Enterprise disaster recovery plan, to involve an implementation of redundant servers in a back up system, which mirrors the primary system. In the event that the primary system goes down, the back up system is still available and becomes the operational system.

It is a best practice to back up BusinessObjects servers on a daily basis.

The Importance of a Proper Back up Sequence

Without backing up the Enterprise system databases and the file repository, no restoration of the environment is possible.

Good back up integrity requires shutting down certain BusinessObjects services prior to capturing the back up. Under certain conditions, failure to follow a proper service shut down sequence before backing up could result in one or both of the following consequences:

- False sense of security in the quality/integrity of the back up

- Inability to fully recover BusinessObjects if the back up is of poor integrity

Enterprise Content Back up compared to Server Back up

Enterprise content back up focuses on the essential components of Enterprise only. With an Enterprise content back up, one can recover a BusinessObjects environment from scratch on a different hardware environment if necessary.

Enterprise content back up does not insure the operating system or any applications, including the Enterprise executables and DLLs; however, it does insure all of the intellectual content that is created and customized by users of the Enterprise system, and that is the most important thing. Content back up also will not insure one against corrupted or deleted Enterprise application DLLs/EXEs or other operating system problems, but these can be resolved by performing a re-installation of operating systems or Enterprise. Enterprise content back ups are relatively fast and inexpensive to capture. This document mostly focuses on a Enterprise content back up strategy.

A server back up is the deepest type of back up. Typically, this is a full back up that captures every byte on every local hard disk in a server. This type of back up insures the server's operating system as well as any applications and data stored on the server's local drives. It is a valuable type of back up, but can also be slow and expensive to capture and later restore. A server back up should incorporate the same data as an Enterprise content back up.

Incremental Back up compared to Full Back up

A full back up captures every targeted byte. Full back ups are the safest and least complex type of back up to restore, but they are also the slowest and most expensive to capture and maintain. Where resources allow, Business Objects advises capturing full back ups once per week.

An incremental back up begins as a full back up. Thereafter, upon each subsequent back up, only the files changed since the last back up are captured. Incremental back ups are faster and less expensive to capture, but they are less robust than full back ups. Because of this, incremental back ups are usually acceptable for daily back ups.

Cold Back up compared to Warm Back up

Cold back ups are a best practice and by far the preferred type of back up to capture on a daily basis. The Central Management Server (CMS) service must be stopped before a true cold back up of the CMS system database and File Repository Server (FRS) can occur. Stopping the CMS will prevent users from accessing the Enterprise system, a factor which must be taken into consideration when scheduling cold back ups.

To aid in stopping and restarting Enterprise XI services before and after a cold back up occurs, it is recommended that two scripts be used, one to stop the relevant services and the other to restart them. These scripts can

be executed before and after the database back up process begins. The UNIX distribution of Enterprise includes the ccm.sh script to assist in the start, stop and restart process.

A warm back up usually allows applications and users to continue to maintain connections to the database and Enterprise XI while the back up occurs. Because of this, a warm back up exposes the possibility that the CMS and Performance Management (PM) tables and FRS will be captured in a state of change; furthermore, the FRS, CMS and PM tables could be captured in an out-of-sync state, a situation which compromises the integrity and usefulness of the back up.

It is recommended to back up the CMS system database and PM repository once daily with incremental back ups and a full back up only once per week. The frequency of back ups may be revised based on an acceptable amount of time for recovery to satisfy your company's requirement.

Business Objects Content to Back up

There are several content-oriented elements that must be backed up daily in order to recover from a disaster. Routinely backing up all of the following content elements will enable you to recover from virtually any type of disaster (virus, hardware failure, natural disaster, and so on).

Database Back up

Central Management Server System Tables

This database contains all the user rights and metadata information about reports and universes, as well as the data connection information. Because the CMS database is the heart of the environment, it is absolutely critical to frequently back up this database. Without this database, the environment cannot be restored. It should be backed up daily.

Performance Management System Tables

This database stores metrics, Key Performance Indexes (KPI), metadata, and key relationships that drive dashboards and scorecards. In many Enterprise environments, these tables will be stored in the same physical database as the CMS system tables, making it easy to capture during a routine back up of the CMS tables. This database should be captured at the same frequency as the CMS system database, ideally on a daily basis.

File Repository

This is a standard OS file share that contains all the report templates and instances for the environment. The file repository typically ranges in size from 1 GB to 100 GB depending on the size and complexity of the deployment. Since the file repository is designed to exist in synchronicity

with the CMS tables, it should be backed up at exactly the same time as the CMS system tables.

Failure to capture the file repository and CMS system tables simultaneously, when the CMS and FRS services are stopped, could result in poor back up integrity. This is because of the increased risk for orphaned report objects or report pointers in the CMS system database if a database restore becomes necessary. Orphaned report pointers are those records in the CMS system database that do not point to a valid input or output file in the Enterprise Input or Output FRS. If a user were to select a report object or report instance that was orphaned, an error message would occur and they would not be able to access that object or instance. Orphaned input or output files in the file repository are a benign problem compared to orphaned pointers in the CMS tables. Only the Input and Output subfolders need to be backed up (the Temp folder can be ignored).

Local audit log files

When auditing servers is enabled, each BusinessObjects server writes audit records to a log file local to the server. At regular intervals, the CMS communicates with the audited servers to request copies of records from the local log files. These log files need to be backed up daily.

Auditing Tables

This database contains usage statistics and auditing information for the environment. A back up of this database is not needed to recover from a disaster because the information this database contains is the least important of all BusinessObjects components.

Custom Java applications/code

Any programmatic customizations to InfoView or other custom user interfaces should be backed up as frequently as they change. During active development periods, these items should be backed up daily. Thereafter, they can be backed up weekly or monthly, or as often as the code is modified. Currently, Business Objects Integrated System consists only of Port Director Dashboards and does not contain any custom code.

The back up and recovery process should be revised once more projects are integrated into it.

Database Connections (ODBC DSNs)

Special database connections (such as ODBC DSNs) can not be easily captured and restored via normal back up processes. Because of this limitation, a back up and recovery plan should cover connectivity parameters for all known data sources. At a minimum, it would cover:

- The name of the ODBC DSN

- The name of the target database

- The type of target database in Oracle

- The user ID and password used to connect to the database

- A listing of the reports that rely on the data source

- Any other pertinent information that an administrator can use to recreate the data source manually if necessary

Query Data Source – Data Warehouse

Although technically not Enterprise components, all reporting databases and cubes should be backed up on a daily basis or at least as frequently as the data changes.

High-Level Sequence of Back up Events

1. The Central Management Server (CMS) and all job-processing and Performance Management servers should be stopped by an automated script. This action:

    i. Releases the CMS' connection to the system database.

    ii. Releases Performance Management's connection to its tables in the CMS system database.

    iii. Prevents users from accessing Enterprise.

    iv. Prevent report jobs/analytics from executing (and terminates any report jobs/analytics already in execution).

    v. Assures the continued integrity of the Enterprise File Store.

2. After the Enterprise services have stopped, the IT Administrator should capture the back up of the components mentioned in the Business Objects Content to Back up section.

3. After the back up is complete, the IT Administrator restarts the Enterprise services. This can be done by an automated script.

High-Level Sequence of Recovery Events

Web and BusinessObjects XI Release 2 System Files

If necessary, rebuild and restore the system, ensuring that the number and size of disk volumes are the same or larger than the previous system. If you must rebuild a system by starting with an empty hard drive, install the OS on the same disk as before, then recreate the partitions and volumes as they were on the damaged system. If

recovering only Enterprise content, make sure to install Enterprise on the same drive as on the original system.

Web and BusinessObjects XI Release 2 Data Files

1. Restore the back up of the CMS system database.

2. Restore the back up of the PM repository.

3. Install/configure the data source client software to point to the restored database and report source.

4. Restore the Input and Output File Repositories.

For replicating on a second server, conduct the installations as above and use the Business Objects Import Wizard to import the required information from one Enterprise system to another.

Individual files from a specific date can be restored from the file system back up tapes. If it is necessary to restore entire file systems, the most recent full system back up tape should be restored first, followed by the first incremental back up, then the second incremental back up, and so on until the file system is fully restored.

▶ www.businessobjects.com