

Oracle® Enterprise Performance Management System

Backup and Recovery Guide

Release 11.1.2.1

Updated: February 2012

EPM System Backup and Recovery Guide, 11.1.2.1

Copyright © 2008, 2012, Oracle and/or its affiliates. All rights reserved.

Authors: EPM Information Development Team

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

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

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

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

U.S. GOVERNMENT RIGHTS:

Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

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

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

Contents

Documentation Accessibility	5
Chapter 1. About Backup and Recovery	7
Assumed Knowledge	7
Installation Documentation Roadmap	7
Repositories, Databases, and File Systems	9
Database Backup Types	9
File System Backup Types	10
Recovery Sequence	11
Chapter 2. Common Backup Tasks	13
Preparing for Backup	13
Database Backup	13
File System Backup	14
Backing Up OS Settings	16
Backing Up Windows Registry Settings	16
System Variable Backup	17
Chapter 3. Foundation Services	19
EPM Workspace and Shared Services	19
Backing Up the File System	19
Restoring EPM Workspace and Shared Services	20
Backing Up the Database	20
Restoring the Database to a Different Server	20
Performance Management Architect	21
Calculation Manager	22
Smart View	22
Chapter 4. Essbase Components	23
Essbase	23
Pre-upgrade Security File Backup	23
Backing Up and Recovering Block Storage Databases	24
Preserving Environment Variable Values	46

Backing Up and Restoring Aggregate Storage Applications	46
Exporting and Importing Partition Definitions	47
Integration Services	47
Essbase Studio	47
Provider Services	48
Chapter 5. Financial Performance Management Applications	49
Planning	49
Business Rules	50
Disclosure Management	50
Financial Close Management	51
Financial Management	51
Performance Scorecard	52
Profitability and Cost Management	53
Strategic Finance	53
Chapter 6. Reporting and Analysis	55
Backing Up the Reporting and Analysis File System	55
Reporting and Analysis Services Suspension	56
Restoring Reporting and Analysis	57
Dashboard Development Services	57
Financial Reporting	58
Production Reporting	58
Chapter 7. Data Management	59
Data Relationship Management	59
FDM	60
ERP Integrator	60
Index	61

Documentation Accessibility

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

Access to Oracle Support

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

1

About Backup and Recovery

In This Chapter

Assumed Knowledge.....	7
Installation Documentation Roadmap	7
Repositories, Databases, and File Systems	9
Recovery Sequence	11

Assumed Knowledge

This guide is for administrators who install, configure, and manage Oracle Enterprise Performance Management System products. It assumes that you have the following skills and knowledge:

- Security and server administration skills
- Windows or UNIX administration skills, depending on your operating system (OS)
- Web application server administration skills
- A strong understanding of your organization's security infrastructure, including authentication providers such as Oracle Internet Directory, Lightweight Directory Access Protocol (LDAP), Microsoft Active Directory, and use of Secure Sockets Layer (SSL)
- Strong relational database management system (RDBMS) administration skills
- A strong understanding of your organization's database and server environments, including file systems
- A strong understanding of your organization's network environment and port usage

Installation Documentation Roadmap

You can find EPM System installation documentation in the [Oracle Documentation Library](http://www.oracle.com/technology/documentation/epm.html) (<http://www.oracle.com/technology/documentation/epm.html>) on Oracle® Technology Network. For faster access to the documentation for a specific release, you can use the Enterprise Performance Management Documentation Portal (<http://www.oracle.com/us/solutions/enterprise-performance-bi/technical-information-147174.html>), which also contains links to EPM Supported Platform Matrices, My Oracle Support, and other information resources.

Note: Always check the [Oracle Documentation Library \(http://www.oracle.com/technology/documentation/epm.html\)](http://www.oracle.com/technology/documentation/epm.html) on Oracle® Technology Network to see whether an updated version of a guide is available.

[Table 1](#) lists the documents to consult for instructions on performing essential installation tasks.

Table 1 Documentation That You Need

Task	Related Documentation
Meeting system requirements and understanding release compatibility	<i>Oracle Hyperion Enterprise Performance Management System Certification Matrix</i> (http://www.oracle.com/technology/software/products/ias/files/fusion_certification.html)
Planning the installation	<i>Oracle Hyperion Enterprise Performance Management System Installation Start Here</i>
<ul style="list-style-type: none">● Installing, configuring, and deploying EPM System products● Starting EPM System products● Validating the installation● Upgrading EPM System products	<i>Oracle Hyperion Enterprise Performance Management System Installation and Configuration Guide</i>
Securing EPM System	<i>Oracle Hyperion Enterprise Performance Management System Security Administration Guide</i>
Provisioning users	<i>Oracle Hyperion Enterprise Performance Management System User and Role Security Guide</i>

[Table 2](#) lists the documents to consult for additional installation tasks that you might need to perform.

Table 2 Documentation That You Might Need

Task	Related Documentation
Troubleshooting installations	<i>Oracle Hyperion Enterprise Performance Management System Installation and Configuration Troubleshooting Guide</i>
Creating a backup of product and application data	<i>Oracle Hyperion Enterprise Performance Management System Backup and Recovery Guide</i>
Migrating from one environment to another	<i>Oracle Hyperion Enterprise Performance Management System Lifecycle Management Guide</i>
Clustering EPM System applications for high availability and disaster recovery	<i>Oracle Hyperion Enterprise Performance Management System High Availability and Disaster Recovery Guide</i>

Additional content is available in the White Papers Library at Oracle Enterprise Performance Management / Business Intelligence White papers. (<http://www.oracle.com/technetwork/middleware/bi-foundation/resource-library-090986.html>).

Repositories, Databases, and File Systems

Many EPM System products use repositories, which contain items that the products require. Repository contents differ by product. Some product repositories use RDBMS, some use file systems, and some use both RDBMS and file systems.

Database Backup Types

You can use several types of database backup, depending on your computing environment.

See http://www.oracle.com/technology/deploy/availability/htdocs/BR_Overview.htm for more information on backup and recovery for Oracle databases.

Physical Backup

Physical backups are copies of physical database files. For example, a physical backup might copy database content from a local disk drive to another secure location.

A physical backup can be hot or cold:

- Hot backup—Users can modify the database during a hot backup. Log files of changes made during the backup are saved, and the logged changes are applied to synchronize the database and the backup copy. A hot backup is used when a full backup is needed and the service level does not allow system downtime for a cold backup.
- Cold backup—Users cannot modify the database during a cold backup, so the database and the backup copy are always synchronized. Cold backup is used only when the service level allows for the required system downtime.

You can perform a full or incremental physical backup:

Note: A cold full physical backup is recommended.

- Full—Creates a copy of data that can include parts of a database such as the control file, transaction files (redo logs), archive files, and data files. This backup type protects data from application error and safeguards against loss by providing a way to restore original data. Perform this backup weekly, or biweekly, depending on how often your data changes. Making full backups **cold**, so that users cannot make changes during the backups, is recommended.

Note: The database must be in archive log mode for a full physical backup.

- Incremental—Captures only changes made after the last full physical backup. The files differ for databases, but the principle is that only transaction log files created since the last backup are archived. Incremental backup can be done **hot**, while the database is in use, but it slows database performance.

In addition to backups, consider using clustering or log shipping to secure database content. See the *Oracle Hyperion Enterprise Performance Management System High Availability Guide* and the RDBMS documentation.

Logical Backup

A logical backup copies data, but not physical files, from one location to another. A logical backup is used to move or archive a database, tables, or schemas and to verify database structures.

A full logical backup enables you to copy these items across environments that use different components, such as operating systems:

- Entire applications
- Data repositories such as the Oracle Hyperion Shared Services Registry and Oracle Essbase cubes
- Individual artifacts such as scripts, data forms, and rule files

A logical export backup generates necessary Structured Query Language (SQL) statements to obtain all table data that is written to a binary file. A logical export backup does not contain database instance-related information, such as the physical disk location, so you can restore the same data on another database machine. Periodic logical export backups (at least weekly) are recommended in case physical backups fail or the database machine becomes unavailable.

Backup with Lifecycle Management

You can use Oracle Hyperion Enterprise Performance Management System Lifecycle Management, which is provided with Oracle Hyperion Foundation Services, to perform logical backups. See the *Oracle Hyperion Enterprise Performance Management System Lifecycle Management Guide*.

File System Backup Types

A complete file system backup includes an entire system directory. For example, backing up the EPM Oracle home directory backs up all installed EPM System products. You can also perform file-system backups of these types and frequencies:

- Post-installation—Directories created or modified if you reconfigure products
- Daily incremental—New directories or files or those modified since the previous day (including repository content and log files)
- Weekly full—All files in the directories for which you perform daily incremental backups
- As needed—Data that is modified infrequently

Recovery Sequence

Restore Oracle Hyperion Shared Services, and the components that you backed up for Shared Services, before restoring other products.

Caution! It is imperative that backup and restore operations for EPM System components be synchronized, because EPM System components continually read and write information to the Shared Services repository. When restoring Shared Services from a backup, for example, you must also restore registered EPM System components from backups that were made at the same time.

2

Common Backup Tasks

In This Chapter

Preparing for Backup	13
Database Backup	13
File System Backup.....	14
Backing Up OS Settings.....	16

Preparing for Backup

Complete these tasks before starting a cold backup:

- Stop products and ensure that all users have logged off.
- Stop all related services. See the *Oracle Hyperion Enterprise Performance Management System Installation and Configuration Guide*.
- Back up the Foundation Services database.

Note: You can also perform hot backups on EPM System products, with some limitations for individual products as described later in this document. These backups must be performed at the same time.

Database Backup

Back up these databases:

- Databases that store EPM System application data
- The Shared Services repository

The Shared Services repository contains the Shared Services Registry, which stores most product configuration settings. It also contains Native Directory, provisioning information, and Oracle Hyperion Enterprise Performance Management Workspace preferences. Oracle recommends a physical full backup immediately after installation and configuration.

For instructions on backing up an individual EPM System component, see the section of this guide that is specific to the component. See [“EPM Workspace and Shared Services”](#) on page 19 for instructions on backing up Foundation Services.

Also back up any database, using the vendor documentation, that you use to store or extract data for use in product applications. Regular backups of database content are recommended for these EPM System components:

- Foundation Services
- Oracle Hyperion Business Rules
- Oracle Hyperion Disclosure Management
- Oracle Hyperion Calculation Manager
- Oracle Hyperion Dashboard Development Services
- Oracle Hyperion Data Relationship Management
- Oracle Hyperion EPM Architect
- Oracle Hyperion Financial Management
- Oracle Hyperion Financial Close Management
- Oracle Hyperion Performance Scorecard
- Oracle Hyperion Planning
- Oracle Hyperion Profitability and Cost Management
- Oracle Hyperion Reporting and Analysis
- Oracle Hyperion Financial Data Quality Management
- Oracle Hyperion Financial Data Quality Management ERP Integration Adapter for Oracle Applications

These products do not use repository databases:

- Oracle Hyperion SQR Production Reporting
- Oracle Hyperion Smart View for Office
- Oracle Hyperion Provider Services
- Disclosure Management

File System Backup

Regular file system backups are recommended for these EPM System products:

- Oracle Hyperion Foundation Services
- Business Rules
- Dashboard Development Services
- Data Relationship Management
- Disclosure Management
- FDM
- Financial Management

- Performance Management Architect
- Oracle Hyperion Performance Scorecard
- Planning
- Profitability and Cost Management
- Reporting and Analysis
- Oracle Hyperion Strategic Finance
- Oracle Hyperion SQR Production Reporting

Oracle recommends daily backup of these items:

- *EPM_ORACLE_INSTANCE/config* (to back up the configuration and reconfiguration settings written to the Shared Services Registry)
- *MIDDLEWARE_HOME/user_projects/domains/domain_name* (EPM System WebLogic domain directory)

Note: This item applies only to products that require a Web application server.

- *EPM_ORACLE_INSTANCE/import_export* (where Oracle Hyperion Enterprise Performance Management System Lifecycle Management content is located)
- Product applications and application data
- In Windows environments:
 - Windows registry: *HKEY_LOCAL_MACHINE* and all of its subkeys

Note: For some EPM System components, you need only back up specific subkeys, as described in the procedures for backing up those components.

Backing up the Windows registry enables system recovery if Windows is reinstalled. See [“Backing Up OS Settings” on page 16](#).

Not applicable for these products:

- Oracle Hyperion SQR Production Reporting Server
- Smart View
- Provider Services

See [“Backing Up OS Settings” on page 16](#).

- *%CommonProgramFiles%/InstallShield/Universal*
- *%USERPROFILE%/oracle.instance*, which enables you to add, remove, reinstall, and upgrade products
- In UNIX environments:
 - *.oracle.instances*, which enables you to add, remove, reinstall, and upgrade products

- \$HOME/InstallShield/Universal
- \$HOME/oraInventory
- Any files such as user profiles, kernel tuning parameters, or .init files that have been edited
- /etc (system-level settings)
- User home directories (user-level settings in hidden files and subdirectories)
- /usr, /lib, and /platform (static system information)
- /var (system logs and spool)

You must back up user home directories and application-specific directories or file systems. Oracle recommends periodically testing the restoration procedure.

Back up the EPM Oracle home directory (to back up all installed products) if you install a new product or apply a patch.

Back up directories and files by copying them to another location. You can also use utilities provided with your OS (such as the Windows 2003 Backup Utility) or other third-party backup utilities. In case of failure, restore these directories and files by returning the copy to the original location.

Backing Up OS Settings

Windows registry settings and specific system variables in Windows and UNIX environments should be backed up.

Backing Up Windows Registry Settings

Backing up the Windows registry (HKEY_LOCAL_MACHINE and its subkeys) enables system recovery if Windows is reinstalled.

Note: For some EPM System components, you need only back up specific subkeys, as described in the procedures for backing up those components.

You can use the Windows `regedit` command to create registry files to back up system and product components. If a failure occurs, you can run the registry files to restore the components.

Note: The following procedure does not apply to Oracle Hyperion SQR Production Reporting Server, Smart View, or Provider Services.

► To back up a component with `regedit`:

1 Select Start and then Run.

- 2 Enter `regedit`, and click **OK**.
- 3 Right-click the subkey for the component in the left panel, and select **Export**.
- 4 Select a location for saving the registry file, enter a file name with the `.reg` extension, and click **Save**.

System Variable Backup

Oracle recommends backing up the `HYPERION_HOME` and `EPM_ORACLE_HOME` system variables.

Note: This recommendation does not apply to Smart View.

3

Foundation Services

In This Chapter

EPM Workspace and Shared Services	19
Performance Management Architect	21
Calculation Manager.....	22
Smart View.....	22

EPM Workspace and Shared Services

EPM Workspace and Shared Services share a file system and database.

Note: You must synchronize Shared Services backups with product backups to preserve provisioning data.

Backing Up the File System

➤ To back up the file system for EPM Workspace and Shared Services:

1 Copy these folders to a storage device or another network location after you install or reconfigure EPM Workspace.

- `EPM_ORACLE_INSTANCE`
- `MIDDLEWARE_HOME/user_projects/domains/domain name`

Note: This is a one-time backup of all Oracle Enterprise Performance Management System components that installed and configured on the machine.

2 Perform a weekly full or daily incremental backup of these subfolders of `EPM_ORACLE_INSTANCE/config`:

- `FoundationServices`
- `Foundation`

Note: The `11.1.2.0` subfolder of `EPM_ORACLE_INSTANCE/config/foundation` contains `.reg.properties`, which is required for recovery.

- 3 **Optional:** Perform a monthly or weekly backup of `MIDDLEWARE_HOME/user_projects/domains/domain name/servers/managed server name/logs`, which contains only historical information.

Restoring EPM Workspace and Shared Services

- To restore EPM Workspace and Shared Services after a failure:
 - 1 Recover all components that you backed up, including Shared Services Registry.
Place the copied directories and files in their original locations.

Note:

- 2 Restart all products and related services.
See the *Oracle Hyperion Enterprise Performance Management System Installation and Configuration Guide*.

Backing Up the Database

- To back up the database for EPM Workspace and Shared Services:
 - 1 Navigate to your database system tables.
 - 2 Back up the Shared Services and EPM Workspace schema if you use Oracle RDBMS; otherwise, back up the SQL Server or DB2 database.

Restoring the Database to a Different Server

If you back up a database from one server and restore it to a second server (for example, because the first database server is under maintenance), you must use the WebLogic Admin Console to update the data source and the `reg.properties` file:

- To restore a database to a different server:
 - 1 Update the data source:
 - a. From the WebLogic Admin Console, select **Services**, then **dataSource**, and then **EPMSysRegistry**.
 - b. On the **Connection Pool** tab, specify the user name, password, and JDBC URL for the second server.
 - c. Click **Save and Activate Changes**.
 - 2 Open `reg.properties` with a text editor and update the user name, password, and JDBC server URL.

The `reg.properties` file is in `EPM_ORACLE_INSTANCE/config/foundation/11.1.2.0`.

3 Start Shared Services.

Performance Management Architect

You should back up the Performance Management Architect database regularly. See “[Database Backup Types](#)” on page 9.

If you change the configuration settings, also back up the file system. See “[File System Backup](#)” on page 14.

► To enable recovery from a failure:

- 1 Back up the Performance Management Architect database and, if necessary, the Performance Management Architect file system as described in [Chapter 2, “Common Backup Tasks.”](#)
- 2 Periodically back up `EPM_ORACLE_HOME/products/Foundation/BPMA/AppServer/DimensionServer/ServerEngine/bin/bpma_server_config.xml`.

► To recover from a failure:

- 1 Restore the Oracle Hyperion EPM Architect database that you backed up.
- 2 To recover configuration settings, restore the file system that you backed up.
- 3 Install Dimension Services Server by running `EPM_ORACLE_HOME/products/Foundation/BPMA/AppServer/DimensionServer/ServerEngine/bin/services_build_helper.exe INSTALL PROD`.
- 4 Create a virtual directory for `hyperion-bpma-server` in Internet Information Services (IIS) that references this folder:

`EPM_ORACLE_HOME/products/Foundation/BPMA/AppServer/DimensionServer/Webservices`

- 5 Ensure that the Microsoft .NET Framework version of the Web application is 2.0, and enable ASP.NET 2.0 Extension.
- 6 Ensure that write access for `C:/Documents and Settings/All Users/Application Data` is enabled for `NETWORK SERVICE` user.
- 7 Run these scripts in `EPM_ORACLE_INSTANCE/bin/deploymentScripts/` `installServiceScripts` to install the J2EE Web tier services:
 - `installServiceEPMDataSync.bat`
 - `installServiceEPMAWebServer.bat`
- 8 Restart the product and any related services.

See the *Oracle Hyperion Enterprise Performance Management System Installation and Configuration Guide*.

Calculation Manager

To enable recovery after a failure, you need only back up the database that you use with Oracle Hyperion Calculation Manager, as described in the RDBMS documentation. Additional precautions that you can take:

- Back up the product components in *EPM_ORACLE_HOME/products/Foundation/CALC*.
- Perform a weekly full or daily incremental backup of *MIDDLEWARE_HOME/user_projects/domains/domain name/servers/managed server name/logs*.

Smart View

- To enable recovery of Smart View after a failure, copy the Microsoft Office documents containing Smart View data to another location.

Include these file types:

- XLS and XLSX (Excel)
 - DOC and DOCX (Word)
 - PPT and PPTX (PowerPoint)
- To recover from a failure, replace the backed up Microsoft Office documents in their original locations.

In This Chapter

Essbase	23
Integration Services.....	47
Essbase Studio.....	47
Provider Services.....	48

Essbase

Regular Essbase backups, which should be integrated into production server maintenance, are key to database maintenance. The volatility of the database and server environment and the need for rapid database restoration if a server interruption occurs should determine backup frequency.

Restore refers to the process of returning a database to the state it was in when a backup was performed. For block storage databases, you can use the automated Essbase backup and restore feature or using manual procedures. For aggregate storage databases, you must use manual backup and restore features.

Recover refers to the process of returning a database to a post-backup state that includes transactions that occurred after the backup was performed. To recover a database, you must use the automated backup and restore and the automated transaction logging and replay features.

For more information about MaxL statements and Administration Services Console options discussed in this section, see the *Oracle Essbase Technical Reference* and *Oracle Essbase Administration Services Online Help*, respectively.

Pre-upgrade Security File Backup

When you upgrade to Essbase 11.1.2.1 from an earlier release, a backup of the security file for the earlier release is created before the security file is upgraded. The security file backup, `Essbase.Bak_preUpgrade`, is in `ARBORPATH/bin`. Unlike `essbase_timestamp.bak`, which regularly backs up the latest state of Essbase security, this pre-upgrade backup file is kept intact and is not updated by further operations.

Backing Up and Recovering Block Storage Databases

To back up and restore block storage databases, use either method:

- Automated database backup and restore and transaction logging and replay

Backup and restore provides the equivalent functionality of manually backing up and restoring a database. When a backed-up database is restored, transactions that occurred after the backup procedure are not recovered. However, with transaction logging and replay, post-backup transactions are captured and can be replayed. Thus, a backed-up database can be recovered to the most-recent state before the interruption occurred.

Using the database backup and restore and transaction logging and replay features eliminates the need for various manual steps and, therefore, enables administrators to back up and recover databases more efficiently. Oracle recommends incorporating these features in your backup and recovery strategy.

See:

- [“Sequence for Fully Recovering Block Storage Databases” on page 24](#)
- [“Using Backup and Restore for Block Storage Databases” on page 25](#)
- [“Using Transaction Logging and Replay For Block Storage Databases” on page 32](#)

- Manual backup and restore

Essbase customers who have designed a backup and restore strategy that uses manual procedures and who do not need the functionality of transaction logging and replay can continue using their manual strategy.

See [“Using Manual Backup and Restore Procedures” on page 39](#).

Sequence for Fully Recovering Block Storage Databases

When you restore a database from a backup, the state of the restored database is exactly as it was when the backup was performed. Any transactions that took place after the backup are not recovered. Transaction logging captures ongoing transactions. These transactions can be replayed to recover the database to its most recent state.

A typical sequence for using these two features is to enable transaction logging and then back up a database. After restoring the backed-up database, you can replay the logged transactions that took place after the backup operation.

Transactions that reset the outline and data together (for example, clearing all loaded data and resetting the outline to empty) can be logged and replayed. See [Table 7 on page 32](#) for a list of transactions that can be logged and replayed.

Outline changes are not logged and, therefore, cannot be replayed. The outline itself, however, is saved as part of a backup. If you change the outline after backing up a database, after restoring the database and before replaying any logged transactions, you must copy the updated outline to the restored database. To avoid having the outline out of sync, Oracle recommends that you back up a database each time you change its outline. If you change a database outline without backing up the database, you should make a manual copy of the changed outline that you can copy it to the restored database before replaying transactions.

[Table 3](#) is an example of how to use these features in tandem.

Table 3 Example Sequence for Using Backup and Restore and Transaction Logging and Replay

Time Period	(Sequence ID) Transaction or Event
T ₀	Enable transaction logging.
T ₁	(1) Perform a data load.
T ₂	(2) Calculate the database.
T ₃	(3) Back up the database.
T ₄	(4) Perform another data load.
T ₅	(5) Update cells in a spreadsheet, and perform a lock and send to update the database.
T ₆	(6) Calculate the database.
T ₇	System failure results in a corrupted database.
T ₈	Restore the backup of the database taken at T ₃ . The restored database includes the results of transactions with sequence IDs of 1 and 2 but not those of 4, 5, and 6.
T ₉	Replay transactions with sequence IDs of 4, 5, and 6. These transactions occurred after the backup was performed at T ₃ and before the database was corrupted at T ₇ , and were not recovered when the database was restored at T ₈ .
T ₁₀	(7) Back up the recovered database.
T ₁₁	Change the database outline.
T ₁₂	(8) Back up the database or manually save the changed outline.

Using Backup and Restore for Block Storage Databases

The backup and restore feature applies to block storage databases.

You must have the Administrator role to back up and restore a database.

In backing up a database, Essbase performs the following tasks:

1. Places the database in read-only mode, protecting the database from updates during the archive process while allowing requests to query the database.
2. Writes a copy of the database files listed in [Table 4](#) to an archive file that resides on the Essbase Server computer.

See [“Configuring and Specifying the Database Archive File” on page 27](#).

3. Returns the database to read-write mode.

[Table 4](#) lists and describes the Essbase database files that are backed up automatically.

Table 4 Essbase Database Files That Are Automatically Backed Up

File	Description
essxxxxx.pag	Essbase data files For example, ess00001.pag
essxxxxx.ind	Essbase index files For example, ess00001.ind
dbname.esm	Essbase Kernel file that contains control and disk volume information used for database recovery
dbname.tct	Transaction control table
dbname.ind	Free fragment file for data and index-free fragments
dbname.otl	Outline file, which stores all metadata for a database and defines how data is stored, but does not store data itself
dbname.otl.keep	Temporary backup of <i>dbname.otl</i> (created by operations that modify the outline and write it to a new file)
x.lro	Linked reporting objects
dbname.otn	Temporary outline file created during a dimension build or outline editing
dbname.db	Database file containing database settings
dbname.ddb	Partition definition file
dbname.ocl	Outline change log created during incremental dimension build
essxxxx.chg	Outline synchronization change log
dbname.alg	Spreadsheet update log that stores spreadsheet update transactions as a unit that can be used as the input source for data loads
dbname.atx	Spreadsheet update log that contains historical information for each transaction, such as user name, date, and timestamp, and the number of transaction rows from the .atx file

In addition to the files that Essbase backs up, you must manually back up the files listed in [Table 5](#). You should back up these files at a later date than when the database backup is performed (for example, a few days after). You should also back up rules files and ESSCMD or MaxL scripts when you create or modify them.

[Table 5](#) lists and describes the Essbase database files that must be backed up manually.

Table 5 Essbase Files That You Must Manually Back Up

File	Description	Location
essbase.sec ¹	Essbase security file	ARBORPATH/bin/
essbase_timestamp.bak	Backup of the Essbase security file	ARBORPATH/bin/
essbase.cfg	Essbase Server configuration file	ARBORPATH/bin/

File	Description	Location
<i>dbname.app</i>	Application file containing application settings	<i>ARBORPATH/app/</i>
.otl .csc .rul .rep .eqd .sel	Database artifact files	<i>ARBORPATH/app/appname/dbname/</i>
ESSCMD or MaxL scripts		No defined storage location

¹Shut down the Agent before backing up *essbase.sec*.

Configuring and Specifying the Database Archive File

In backing up a database, Essbase copies the database files to an archive file, which must reside on the Essbase Server computer. When specifying the archive file name and location, follow these guidelines:

- Provide the full path to a directory on Essbase Server and the name of the archive file.
If only the archive file name is provided, Essbase writes the archive file to *ARBORPATH/app*.
- Oracle recommends writing the archive file to a disk other than the one where *ARBORPATH* is located.
- Oracle recommends naming the archive file with an *.arc* extension.
- The archive file size corresponds to the size of the database you back up and is limited only by disk space, unless you split the archive file into multiple files. (See [“Splitting the Archive File Into Multiple Files” on page 28](#).) With the single-file configuration, Oracle recommends saving archive files to a file system that supports large files.

For Windows, the file system must be formatted as NTFS. For UNIX, large file support must be enabled; also, use the *ULIMIT* setting to specify a file size for the archive file. If you set *ULIMIT* to a specific file size, ensure that the value is sufficiently large, based on the size of the database, or set *ULIMIT* to unlimited. See your OS documentation.

- When backing up a database to an archive file, use *force* option to overwrite the archive file; otherwise, the operation fails.

Caution! Before using the *force* option, ensure that you no longer need the current archive file contents.

Splitting the Archive File Into Multiple Files

By default, Essbase creates one large archive file. If you cannot use large files in your environment, or if your file-transfer tools cannot handle large files, you can configure Essbase to split the archive into multiple files of 2 GB or less: In the `essbase.cfg` file, set the `SPLITARCHIVEFILE` configuration to `TRUE`.

The first (or main) archive file that Essbase creates uses the file name that you specify (for example, `samplebasic.arc`). When the main archive file reaches the 2 GB limit, Essbase creates another file. In naming each successive archive file, Essbase increments the main archive file name with “_n”, where *n* is an integer (starting with 1). For example, three archive files created to back up the Sample.Basic database would be named as follows:

```
samplebasic.arc
samplebasic_1.arc
samplebasic_2.arc
```

All split archive files are created in the directory that you specified when specifying the file name and location of the main archive file.

Note: When restoring a database in which the archive is split into multiple files, Essbase looks for multiple archive files even if, after the backup, you set `SPLITARCHIVEFILE` to `FALSE` for that database. Also, Essbase expects all archive files for a database to be in the same directory.

Backing Up Block Storage Databases

To back up a database, you must have the Administrator role.

➤ To back up a database, use one of these tools:

- Oracle Essbase Administration Services

See “Backing Up Block Storage Databases” in *Oracle Essbase Administration Services Online Help*.

In Administration Services Console, use the **Archive Database** command.

- MaxL

See “Alter Database” in the *Oracle Essbase Technical Reference*

In MaxL, use the **alter database** statement with the **archive to file** grammar. The syntax for the statement:

```
alter database apptime.dbname [force] archive to file BACKUP-FILE;
```

For example, the following statement backs up the Sample.Basic database to the specified archive file on Essbase Server:

```
alter database Sample.Basic archive to file '/Oracle/samplebasic.arc';
```

If the `samplebasic.arc` file exists on Essbase Server, use **force** grammar to overwrite the file contents. Example:

```
alter database Sample.Basic force archive to file '/Oracle/  
samplebasic.arc';
```

Note: At a different time from when you back up the database, manually back up the files listed in [Table 5 on page 26](#).

Retrieving Archive File Information

Essbase can retrieve the following information about the backed-up database from the archive file:

- Overview information:
 - Application name
 - Database name
 - Archive time
- Disk volume names

➤ To retrieve archive file information, use the **query archive_file** MaxL statement.

The syntax for the statement:

```
query archive_file BACKUP-FILE [get overview] [list disk volume];
```

In the MaxL Script Editor in Administration Services Console, you can view the results of the query. [Figure 1](#) shows overview information:

Figure 1 Archive File Overview Information

Application	Database	Backup Time
Sample	Basic	Thu Apr 03 10:54:21 2008

[Figure 2](#) shows disk volume names:

Figure 2 Archive File List of Disk Volumes

Volume
C

You can also view disk volume information in Administration Services Console when using the **Restore Database** command.

Note: On Windows, Essbase adds the default ARBORPATH drive (for example, the C: drive) as a disk volume, even if the database that you backed up does not store data on that disk volume. See [“Working with Disk Volumes” on page 31](#).

Restoring Block Storage Databases

You must have the Administrator role to restore a database.

Before restoring the database, you should terminate active client connections to the database.

In restoring a database, Essbase empties the database and locks it. Before extracting the contents of the archive file, Essbase validates the file. Essbase then copies index and page files to the specified disk volumes and updates `dbname.esm` with disk volume information. See [“Working with Disk Volumes” on page 31](#).

If you have configured Essbase to split the archive file into multiple files (see [“Configuring and Specifying the Database Archive File” on page 27](#)), you must specify only the file name of the main archive file that you want to restore (for example, `samplebasic.arc`).

Note: When restoring a database in which the archive file is split into multiple files, Essbase looks for multiple archive files, even if, after the backup, you set `SPLITARCHIVEFILE` to `FALSE` for that database. Also, Essbase expects all of a database's archive files (main and split) to be in the same directory.

► To restore a database, use a tool:

Tool	Topic	Location
Administration Services	Restoring Block Storage Databases	<i>Oracle Essbase Administration Services Online Help</i>
MaxL	alter database	<i>Oracle Essbase Technical Reference</i>

In Administration Services Console, use the **Restore Database** command.

In MaxL, use the **alter database** statement with the **restore from file** grammar. The syntax for the statement:

```
alter database appname.dbname [force] restore from file BACKUP-FILE
[replace disk volume VOL];
```

Typically, you restore a database to the application and database from which the backup was taken. Therefore, the names in the archive file of the backed-up database and its associated application, which are to be restored, are the same. However, if the names of the backed-up database and application differ from the application and database to which you are restoring data, you must use **force** grammar. Statement syntax:

```
alter database appname.dbname force restore from file BACKUP-FILE;
```

For example, you can use the backup for Sample.Basic to restore to Sample.New (the database name is different), MyCompany.Basic (the application name is different), or MyCompany.New (both names are different).

See [“Retrieving Archive File Information” on page 29](#).

Restoring Manually Backed-Up Files

After restoring a backed-up database, you typically need not restore the files that you manually backed up (see [Table 5 on page 26](#)).

Restore manually backed up files in these situations:

- If a server interruption corrupted any files, such as security files
- If you encounter problems (such as missing rules files or scripts) when replaying logged transactions

Working with Disk Volumes

You can install Essbase on one disk volume and store index files (*essn.ind*), and data files (*essn.pag*) on one or more other disk volumes. Disk volume information is saved in the *dbname.esm* file and is used when restoring a database to ensure that the index and data files are copied to the correct disk volumes.

Even if you change the disk volumes that a database uses, all currently and previously used disk volume information remains in the database files. When retrieving disk volume information from the database archive file or viewing disk volume information in Administration Services Console or in the MaxL Shell, Essbase lists all the disk volumes that have been associated with the database. Additionally, Essbase lists the default ARBORPATH drive (for example, on Windows, the C: drive, if ARBORPATH resides on C:) as a disk volume. See [“Retrieving Archive File Information” on page 29](#).

When restoring a database, you can replace disk volume names; however, the number of disk volumes must be the same, and the space required must at least the same, as those for the database before it was backed up.

In Administration Services Console, use the **Advanced** option in the Restore Database dialog box to replace the disk volume names.

When using the **alter database** MaxL statement with the **replace disk volume VOL** grammar, the valid values for the VOL argument are a comma-separated list of volumes to replace:

- 'VOL1' with 'VOL2'
- 'VOL3' with 'VOL4'
- 'VOL5' with 'VOL6'

For example, the following statement restores the Sample.Basic database using the *samplebasic.arc* archive file and replaces the specified disk volumes:

```
alter database Sample.Basic restore from file '/Oracle/samplebasic.arc'  
replace disk volume 'C' with 'F', 'D' with 'G', 'E' with 'H';
```

Working with Unicode and Non-Unicode Applications

When working with Unicode and non-Unicode applications, Essbase does not allow a backed-up database from a Unicode application to be restored to a non-Unicode application.

Table 6 lists the supported combinations of restoring backed-up databases between Unicode and non-Unicode applications.

Table 6 Combinations of Backed Up and Restored Databases by Unicode and Non-Unicode Application Modes

Backed Up From	Restored To	Supported
Unicode	Unicode	Yes
Unicode	Non-Unicode	No
Non-Unicode	Non-Unicode	Yes
Non-Unicode	Unicode	Yes

Backing Up and Restoring Partitioned Databases

When backing up and restoring partitioned databases, follow these guidelines:

- Back up and restore the source and target databases simultaneously.
- If you restore a database to an application or database whose names are not the same as the names of the application or database that you backed up, you must redefine the partition. See the *Oracle Essbase Database Administrator's Guide*.

Using Transaction Logging and Replay For Block Storage Databases

To facilitate recovering a block storage database to a later time than a restored database, you must enable transaction logging. As transactions are executed, Essbase writes operational parameters to a log store. Users with the Essbase Administrator role can view a list of logged transactions and then replay them to recover the data that was not captured after a backed-up database is restored.

Table 7 lists the transactions, by category, that Essbase logs when transaction logging is enabled:

Table 7 List of Logged Transactions by Category

Category	Transaction
Calculation	<ul style="list-style-type: none">● Execute the default or server-side calculation.● Execute a client-side calculation.
Data load	<ul style="list-style-type: none">● Import data from different sources to Essbase Server.● Clear all loaded data and reset the outline to empty.● Clear all loaded data.● Execute a client-side data load.
Lock and send	Update database cells with data from Smart View or Oracle Essbase Spreadsheet Add-in.

The operational parameters that are logged for each transaction vary. Table 8 shows the parameters that are logged for three representative transactions:

Table 8 Examples of Parameters Logged for Specific Transactions

Transaction	Logged Parameters
Execute a client-side calculation	<ul style="list-style-type: none"> ● User who submitted the request ● Start time ● End time ● Sequence ID ● RequestType ● Calculation script contents
Import data from different sources to Essbase Server	<ul style="list-style-type: none"> ● User who submitted the request ● Start time ● End time ● Sequence ID ● RequestType ● Rule file name and location ● Data file name and location ● If SQL source, the SQL connection information ● If the data and rule files are on the client computer, archive the files to the <code>Replay</code> directory. The directory path is logged for use during the replay operation. <p>Essbase autogenerates a unique file name for archived data and rule files, such as <code>98761234.txt</code> and <code>98761234.rul</code>.</p>
Update database cells with data from Smart View, or Oracle Essbase Spreadsheet Add-in	<ul style="list-style-type: none"> ● User who submitted the request ● Start time ● End time ● Sequence ID ● RequestType ● Essbase tracks information about changed cells

Note: “Replay” is a reserved word and cannot be used as the name of a block or aggregate storage database. If you named a database “replay” in the past, you must rename the database before enabling the transaction logging and replay feature.

Enabling Transaction Logging

Transaction logging can be enabled at the server, application, or database level.

To enable transaction logging, you must specify a centralized location where Essbase can write transaction log stores. The location must be to an existing directory on Essbase Server.

Add the `TRANSACTIONLOGLOCATION` configuration setting to `essbase.cfg`. The syntax for the statement:

```
TRANSACTIONLOGLOCATION [appname [dbname]] LOGLOCATION NATIVE ENABLE |
DISABLE
```

Note: Do not change the NATIVE argument, which is a reserved field. For the log location, Oracle recommends using a physical disk other than the disk on which the ARBORPATH directory or disk volumes reside.

In *LOGLOCATION*, Essbase creates subdirectories corresponding to the applications and databases for which you enable transaction logging, using the following structure:

LOGLOCATION/appname/dbname

For example, the following statement enables transaction logging for all databases associated with the Sample application:

```
TRANSACTIONLOGLOCATION Sample /Oracle/trlog NATIVE ENABLE
```

As transactions are logged for the Sample.Basic database, the log store is written to:

/Oracle/trlog/Sample/Basic

Depending on the number of databases for which you enable transaction logging, you might want to create more than one centralized transaction log location; however, Oracle recommends keeping the number of log locations to a minimum.

Additionally, by using multiple TRANSACTIONLOGLOCATION statements, you can enable transaction logging at a more global level and, at the same time, disable logging at a more granular level. In the *essbase.cfg* file, for the override to take effect, the more global enabling statement must precede the more granular disabling statement.

Consider the following examples:

- The first statement enables transaction logging for all applications and their associated databases on Essbase Server; the second statement disables transaction logging for all databases associated with a specific application (Sample):

```
TRANSACTIONLOGLOCATION /Oracle/trlog NATIVE ENABLE
```

```
TRANSACTIONLOGLOCATION Sample /Oracle/trlog NATIVE DISABLE
```

- The first statement enables transaction logging at the application level (Sample); the second statement disables transaction logging for a specific database (Basic) in the application:

```
TRANSACTIONLOGLOCATION Sample /Oracle/trlog NATIVE ENABLE
```

```
TRANSACTIONLOGLOCATION Sample Basic /Oracle/trlog NATIVE DISABLE
```

Note: Before renaming or copying an application or database for which transaction logging is enabled, you must enable logging for the renamed or copied application or database and specify the same LOGLOCATION that is specified for the source application and database.

Configuring Transaction Replay

To enable the replay of logged transactions, Essbase creates archive copies of data load and rules files in *ARBORPATH/app/appname/dbname/Replay*.

By default, Essbase archives only data load and rules files for client data loads.

To change the type of data to be archived, add the TRANSACTIONLOGDATALOADARCHIVE configuration setting to the `essbase.cfg` file. The syntax for the statement:

```
TRANSACTIONLOGDATALOADARCHIVE [appname [dbname]] [OPTION]
```

Valid values for the `OPTION` argument:

- **CLIENT**—(Default) Archives data load and rules files for client data loads.
- **SERVER**—Archives data load and rules files on the server and SQL-server data loads.

Caution! Server data loads are replayed using the data load and rules files that are archived on the server in the `Replay` directory. Do not rename these files. Also, if the contents of the data load and rules files are changed before the replay operation, the modified data is used during replay. Therefore, the data in the recovered database will not be the same as the original data.

- **SERVER_CLIENT**—Archives server and client data.
- **NONE**—No data is archived.

If you select **NONE** and you use client data, Essbase cannot replay the data load. To recover transactions, you must manually load the client data before you replay the remaining transactions.

Caution! If you use server or SQL data and the data and rules files are not archived in the `Replay` directory (for example, you did not use the **SERVER** or **SERVER_CLIENT** option), Essbase replays the data that is in the data source, which may or may not be the data that was originally loaded.

For example, the following statement archives server and client data for all databases on Essbase Server:

```
TRANSACTIONLOGDATALOADARCHIVE SERVER_CLIENT
```

Viewing Logged Transactions

An administrator can view the list of logged transactions and the information associated with each transaction. You can specify whether to list transactions that were logged after the following conditions:

- A specified time
- The time when the last replay request was executed or the time of the last restored backup (whichever occurred later)

➤ To view logged transactions, use a tool:

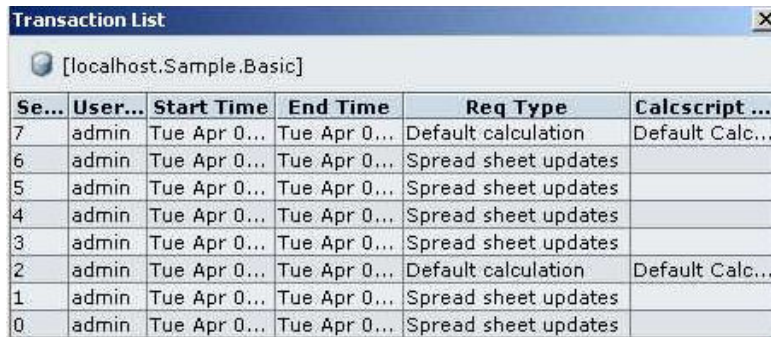
Tool	Topic	Location
Administration Services	Viewing Logged Transactions for Block Storage Databases	<i>Oracle Essbase Administration Services Online Help</i>

Tool	Topic	Location
MaxL	query database	Oracle Essbase Technical Reference

In Administration Services Console, use the **Display Transactions** command to view a list of transactions, as shown in [Figure 3](#). You can sort the list by the following attributes:

- Sequence ID
- Username
- Start Time
- End Time
- Request Type

Figure 3 List of Logged Transactions



Se...	User...	Start Time	End Time	Req Type	Calcscript ...
7	admin	Tue Apr 0...	Tue Apr 0...	Default calculation	Default Calc...
6	admin	Tue Apr 0...	Tue Apr 0...	Spread sheet updates	
5	admin	Tue Apr 0...	Tue Apr 0...	Spread sheet updates	
4	admin	Tue Apr 0...	Tue Apr 0...	Spread sheet updates	
3	admin	Tue Apr 0...	Tue Apr 0...	Spread sheet updates	
2	admin	Tue Apr 0...	Tue Apr 0...	Default calculation	Default Calc...
1	admin	Tue Apr 0...	Tue Apr 0...	Spread sheet updates	
0	admin	Tue Apr 0...	Tue Apr 0...	Spread sheet updates	

Although you can sort the list of transactions, you must replay transactions in the same order as the sequence ID.

When using the **query database** MaxL statement with the **list transactions** grammar, you can specify whether to display the list output in the MaxL Shell window (the default) or to write the list output to a specified file. The syntax for the statement:

```
query database appname.dbname list transactions [after TIME [[force]
write to file FILE-NAME]]];
```

For example, the following statement displays, in the MaxL Shell window, the transactions in the Sample.Basic database that were logged after the last replay request was executed or after time of the last restored backup (whichever occurred later):

```
query database Sample.Basic list transactions;
```

Writing the output to a file is useful for processing the log information with other tools. For example, you can import the file contents into a relational database and write a tool to analyze the information.

When using the **write to file** grammar, the list output is written to a comma-separated file on the Essbase Server computer. Provide the full path to an existing directory on Essbase Server and the name of the output file. If only the output file name is provided, Essbase writes the file to *ARBORPATH/app*.

When writing to an existing output file, use **force** grammar to overwrite the file.

For example, the following statement writes Sample.Basic database transactions that were logged after November 20, 2009, at 12:20:00 to a CSV file in the Sample.Basic database directory:

```
query database Sample.Basic list transactions after '11_20_2009:12:20:00' write to file EPM_ORACLE_HOME/products/Essbase/EssbaseServer/app/Sample/Basic/listoutput.csv';
```

Configuring User Security for Replaying Logged Transactions

In replaying logged transactions, by default, Essbase uses the security settings of the user who originally performed the transaction. If that user no longer exists or if the user's user name is changed, the replay operation fails. To use the security settings of the administrator who performs the replay operation (either explicitly or if the original user's settings cannot be used), use the `REPLAYSECURITYOPTION n` configuration setting in `essbase.cfg`. Values for *n* and whose security settings they specify:

- 1—(default) The user who originally performed the transaction
- 2—The administrator performing the replay operation
- 3—The user who originally performed the transaction

If that user no longer exists or that user's user name was changed, the security settings of the administrator performing the replay operation are used.

Replaying Logged Transactions

Only an administrator can replay transactions. You can replay logged transactions based on these criteria:

- Transactions logged after a specified time
- Transactions logged after the last replay request was executed or after the time of the last restored backup (whichever occurred later)
- Selectively, transactions based on a range of sequence IDs

Each logged transaction is assigned a sequence ID, indicating the order in which the transaction was performed. To ensure the integrity of the restored data after a replay, Essbase enforces the replay of transactions in the same order in which they were originally performed. For example, if a data load was followed by a calculation, replaying the calculation before the data load would produce incorrect results; the data load transaction must be replayed before the calculation transaction.

The order of sequence IDs is tracked across multiple replay commands. After a transaction is replayed, you can replay only transactions with a greater sequence ID. For example, after replaying transactions with sequence IDs of 1, 2, and 3, you can replay only transactions with a sequence ID of 4 or greater.

Transactions that are executed and logged after the restore operation are not replayed, unless you replay those transactions using their sequence IDs. After restoring a database, Oracle

recommends that you finish replaying the transactions that were logged after the backup and before the restore and that are needed to fully recover the database; then you can continue executing new transactions.

Note: You can skip replaying a transaction if you are sure that the transaction results are not required to recover the database. For example, if you performed two full data loads with identical data, you need only replay one of the data loads.

► To replay logged transactions, use a tool:

Tool	Topic	Location
Administration Services	Replaying Logged Transactions for Block Storage Databases	<i>Oracle Essbase Administration Services Online Help</i>
MaxL	alter database	<i>Oracle Essbase Technical Reference</i>

The replay functionality is the same whether you use Administration Services Console or MaxL.

To selectively replay transactions, enter a comma-separated string of sequence ID ranges. A range can consist of one or more transactions:

- One transaction: n to n ; for example, 1 to 1
- Multiple transactions: x to y ; for example, 20 to 100

In Administration Services Console, use the **Replay Transactions** command.

In MaxL, use the **alter database** statement with the **replay transactions** grammar. Syntax:

```
alter database appname.dbname replay transactions [after TIME] [using  
sequence_id_range COMMA-SEPARATED_RANGE];
```

For example, the following statement replays the transactions in the Sample.Basic database with sequence IDs 1–10 and 20–100:

```
alter database Sample.Basic replay transactions using sequence_id_range  
1 to 10,20 to 100;
```

Removing Transaction Log Store and Archived Replay Data Files

Periodically, you might want to remove the transaction log store and the files in the Replay directory to increase available disk space on Essbase Server.

Transaction log store: Oracle recommends removing the transaction log store for one database at a time. The log store is in a subdirectory under the log location specified by the TRANSACTIONLOGLOCATION configuration setting. For example, if the log location for the Sample.Basic database is /Oracle/trlog, delete the contents of /Oracle/trlog/Sample/Basic

See [“Enabling Transaction Logging” on page 33](#).

Replay directory: After you have replayed transactions, the data and rules files associated with the replayed transactions can be removed from the `ARBORPATH/app/appname/dbname/Replay` directory (see [“Configuring Transaction Replay” on page 34](#)). You can delete all of the files in the Replay directory, or follow these guidelines for selectively removing files:

- Remove the data and rules files in chronological order, from earliest to latest.
- Do not remove data and rules files with a timestamp that is later than the timestamp of the most recent archive file.

Note: Oracle recommends waiting until after several subsequent database backups before deleting files associated with transaction logging and replay.

Using Transaction Logging and Replay with Partitioned Databases

When logging and replaying transactions from partitioned databases, follow these guidelines:

- Partition commands (for example, synchronization commands) are not logged and, therefore, cannot be replayed. When recovering a database, you must replay logged transactions and manually make the same partition changes in the correct chronological order.
- When using partitioned databases or using the `@XREF` function in calculation scripts, you must selectively replay logged transactions in the correct chronological order between the source and target databases.

Note: Back up and restore the source and target databases simultaneously. See [“Backing Up and Restoring Partitioned Databases” on page 32](#).

Using Manual Backup and Restore Procedures

If you have designed a backup and recovery strategy using manual procedures, you can continue using them. Oracle, however, recommends that you incorporate backup and restore (see [“Using Backup and Restore for Block Storage Databases” on page 25](#)) and transaction logging and replay (see [“Using Transaction Logging and Replay For Block Storage Databases” on page 32](#)) into your backup and recovery strategy.

See these topics for manually backing up and restoring block storage databases:

- [“Backing Up and Restoring Database Files” on page 39](#)
- [“Backing Up Files During Runtime” on page 40](#)
- [“Backing Up and Restoring Data” on page 42](#)

Backing Up and Restoring Database Files

Regularly back up the server, application, and database files listed in [Table 9](#). Typically, you should perform a file backup after Essbase applications and databases, and the Agent, are shut down.

Table 9 Essbase Files to Back Up

File	Description	Location
essxxxxx.ind ¹	Essbase index file	ARBORPATH/app/appname/dbname/
essxxxxx.pag ²	Essbase data file	ARBORPATH/app/appname/dbname/
dbname.esm	Essbase Kernel file that contains control information used for database recovery	ARBORPATH/app/appname/dbname/
dbname.tct	Transaction control table	ARBORPATH/app/appname/dbname/
dbname.ind	Free fragment file for data and index free fragments	ARBORPATH/app/appname/dbname/
dbname.otl	Outline file, which stores all metadata for a database and defines how data is stored, but does not store data itself	ARBORPATH/app/appname/dbname/
dbname.app	Application file containing application settings	ARBORPATH/app/
dbname.db	Database file containing database settings	ARBORPATH/app/appname/dbname/
x.lro	Linked reporting objects	ARBORPATH/app/appname/dbname/
essbase.sec ³	Essbase security file	ARBORPATH/bin/
essbase_timestamp.bak	Backup of the Essbase security file	ARBORPATH/bin/
essbase.cfg	Essbase Server configuration file	ARBORPATH/bin/
.otl .csc .rul .rep .eqd .sel	Database artifact files	ARBORPATH/app/appname/dbname/
ESSCMD or MaxL scripts		No defined storage location

¹Back up all .ind files related to a database, because a database may have multiple .ind files.

²Back up all .pag files related to a database, because a database may have multiple .pag files.

³Shut down the Agent before backing up essbase.sec.

When performing a file system backup, use the file system backup software of your choice. You can back up specific directories or files or the entire Essbase directory structure. Back up data on every disk volume.

To restore a database, ensure that the application is stopped and replace the files on disk with the corresponding backed up files.

Backing Up Files During Runtime

If any Essbase databases must be running at the time of the backup, follow these steps:

1. [“Putting a Database in Read-Only Mode” on page 41](#)
2. [“Performing a File Backup” on page 41](#)
3. [“Returning a Database to Read-Write Mode” on page 42](#)
4. [“Restoring the File Backup” on page 42](#)

Putting a Database in Read-Only Mode

Putting the database in read-only (or archive) mode protects it from updates during backup.

► To put a database in read-only mode, use a tool:

Tool	Topic	Location
MaxL	alter database begin archive	<i>Oracle Essbase Technical Reference</i>
ESSCMD	BEGINARCHIVE	<i>Oracle Essbase Technical Reference</i>

After performing the backup, return the database to read-write mode.

The `BEGINARCHIVE` command performs the following tasks:

- Commits modified data to disk.
- Switches the database to read-only mode.
- Reopens the database files in shared, read-only mode.
- Creates, in the `ARBORPATH/app/appname/dbname` directory, a file (default name `archive.lst`) that lists files to be backed up.

Attempting to modify data during the backup process results in an error message that data is in read-only mode.

Begin archive does not perform the backup; it protects the database during backup. If you cancel the `BEGINARCHIVE ESSCMD` command or the `alter database begin archive` MaxL statement, and you receive a “can’t cancel” message, the system may be in the final stage of writing items to the drive, when the operation cannot be canceled.

Caution! If you back up data without using `BEGINARCHIVE`, ensure that all Essbase applications are closed and that all users are logged off during the backup, to avoid corrupting the database.

Performing a File Backup

Put the database in read-only mode before you perform the backup.

- To back up data, use a third-party backup utility to back up the files listed in `archive.lst` and in [Table 9, “Essbase Files to Back Up,” on page 40](#), or back up the entire Essbase directory structure.

Returning a Database to Read-Write Mode

After performing a backup, return the database to read-write mode.

- To return the database to read-write mode, use a tool:

Tool	Topic	Location
MaxL	alter database end archive	<i>Oracle Essbase Technical Reference</i>
ESSCMD	ENDARCHIVE	<i>Oracle Essbase Technical Reference</i>

The end-archive utility performs the following actions:

- Returns the database to read-write mode.
- Reopens database files in exclusive, read-write mode.

Note: You must use the end-archive utility to put the database back into read-write mode, even if you shut down and restart the database. The end-archive utility does not restart the database.

Restoring the File Backup

To restore a database, replace the files on disk with the corresponding files from the backup.

The application should be stopped unless you are restoring from an export file. In that case, ensure that the application is not accepting client connections.

Backing Up and Restoring Data

Exporting data copies the data to a file that you specify.

When you export data to a text file, the data is not compressed. The text export file contains only data; it does not include control, outline, or security information.

Consider exporting data to accomplish the following tasks:

- Transfer data across platforms
- Back up only part of the data; for example, level-0 blocks
- Create an exported file in text format rather than binary format

The advantages of exporting data:

- You can use text export files to load data from the source database into databases on other platforms. Exporting a database in column format enables you to manipulate the export file and use it with a rules file to load the data back or to another database.

Loading an export file into a database fails if the database outline does not contain all the members found within the export file.

If the outline changes between the time that the export file is created and reloaded (and the new outline contains all the members found within the export file), the load time might be significantly longer than if the outlines were identical.

- Data integrity is verified because every block is checked to confirm whether corresponding page and index files match.
- Exporting data, clearing all data from the database, and reloading the text file can reduce fragmentation.

The disadvantages of exporting data:

- Unless dynamic calculations are executed at the time of the export, only stored data and data from previously calculated Dynamic Calc and Store members are included in the export.
- During a database export, users cannot write to the database. After an export has started, users can do read operations. Exports of large databases require considerable time, during which users can only read the data.

Note: You can export subsets of data by creating reports or calculation scripts. Using calculation scripts, you can export data to text or binary files, or directly into a relational database. See the *Oracle Essbase Database Administrator's Guide*.

Exporting Data

The same basic information is required, regardless of the method used to export data:

- Names of export data files
- The amount of data to export
 - All data
 - Level-0 blocks only (blocks containing only level-0 sparse member combinations; these blocks may contain data for upper-level dense dimension members)
 - Data from input blocks only (blocks containing data from a previous data load or spreadsheet lock and send)
- Whether to export data in a columnar or noncolumnar format

In each row, the columnar format displays a member name from every dimension. Names can be repeated from row to row.

The columnar format provides a structure to the exported data, so that it can be used for further data processing by applications other than Essbase tools; for example, relational databases. In noncolumnar format, sparse members identifying a data block are included only once for the block. Because the export file in noncolumnar format is smaller than in columnar format, reloading a file in noncolumnar format is faster.

► To export data, use a tool:

Tool	Topic	Location
Administration Services	Exporting Databases	<i>Oracle Essbase Administration Services Online Help</i>
MaxL	export data	<i>Oracle Essbase Technical Reference</i>
ESSCMD	EXPORT or PAREXPORT	<i>Oracle Essbase Technical Reference</i>
Report Writer	Use a Report Writer script to export selected data.	<i>Oracle Essbase Database Administrator's Guide</i>
Calculation script (block storage only)	DATAEXPORT calculation commands	<i>Oracle Essbase Technical Reference</i>

Note: To improve export performance, you can export data in parallel to a specified number of files.

Exporting Files Larger Than 2 GB

Some file systems do not support text files larger than 2 GB. On any OS, if Essbase anticipates that an export file exceeds 2 GB, it creates two or more export files, as needed. The requested file name for the main file is used. An underscore and a sequential cardinal number are appended to the names of the additional files, starting with _1. For example, if the requested file name is `expJan.txt`, and the exported data would exceed 4 GB, Essbase creates three files, naming them `expJan.txt`, `expJan_1.txt`, and `expJan_2.txt`. Exported data files can be reloaded in any sequence.

Restoring the Data Backup

When you reload data that has been exported, it is marked as input data. If you reload data exported from level-0 blocks or input blocks, you must recalculate the database after reloading. When Essbase recalculates the database, it recalculates every data block.

If you export all data in a database and then reload, Essbase marks all blocks in the database as input blocks. Consequently, you cannot clear data, because the database does not contain noninput blocks.

When you reload data that has been exported, Essbase also marks the data blocks as dirty. If you calculated the database before exporting it, to save time during the next calculation, set the status of the blocks as clean. If you did not calculate the database before exporting it, you need not set the status of the blocks as clean.

► To reload exported data, use a tool:

Tool	Topic	Location
Administration Services	Performing a Data Load or Dimension Build	<i>Oracle Essbase Administration Services Online Help</i>
MaxL	import data	<i>Oracle Essbase Technical Reference</i>

Tool	Topic	Location
ESSCMD	IMPORT	<i>Oracle Essbase Technical Reference</i>
Calculation script	DATAIMPORTBIN (exported binary files only)	<i>Oracle Essbase Technical Reference</i>

- To clean block status in a database after exporting all data and reloading, run the following calculation script:

```
Set ClearUpdateStatus Only;
Calc All;
```

Maintaining LRO Links

LROs (linked reporting objects) are not restored with backed-up databases; therefore, you must export them and then import them.

As part of your database backup procedure, export the LROs.

- To export LRO links, use a tool:

Tool	Topic	Location
Administration Services	Exporting LROs	<i>Oracle Essbase Administration Services Online Help</i>
MaxL	export lro	<i>Oracle Essbase Technical Reference</i>

As part of your database restore procedure, import the LROs that you previously exported.

- To import LRO links, use a tool:

Tool	Topic	Location
Oracle Essbase Administration Services	Importing LROs	<i>Oracle Essbase Administration Services Online Help</i>
MaxL	import lro	<i>Oracle Essbase Technical Reference</i>

Resolving Corrupt Database Files

The database does not start on Essbase Server if database files are corrupt.

- To restore a corrupt database:

1 Delete these files:

- `essxxxxx.pag`
- `dbname.esm`
- `essxxxxx.ind`

- `dbname.tct`
- `dbname.ind`

- 2 Restart the database.
- 3 Reload from data or export files that you created before the corruption.

Preserving Environment Variable Values

Note the values of the `ARBORPATH` and `ESSLANG` environment variables.

Backing Up and Restoring Aggregate Storage Applications

The file structure described in [Table 10](#) is unique to aggregate storage applications.

Table 10 Aggregate Storage Application Files

Directory or File	Description	Location
<code>appname</code>	Application directory	<code>ARBORPATH/app/appname</code>
<code>appname.app</code>	Application file containing application settings	<code>ARBORPATH/app/appname/</code>
<code>appname.log</code>	Application log file	<code>ARBORPATH/app/appname/</code>
<code>dbname</code>	Database directory	<code>ARBORPATH/app/appname/dbname</code>
<code>dbname.db</code>	Database file containing database settings	<code>ARBORPATH/app/appname/dbname/</code>
<code>dbname.dbb</code>	Backup of database file	<code>ARBORPATH/app/appname/dbname/</code>
<code>dbname.ddb</code>	Partition definition file	<code>ARBORPATH/app/appname/dbname/</code>
<code>dbname.otl</code>	Outline file	<code>ARBORPATH/app/appname/dbname/</code>
<code>dbname.otl.keep</code>	Temporary backup of <code>dbname.otl</code> (created by operations that modify the outline and write it to a new file.)	<code>ARBORPATH/app/appname/dbname/</code>
<code>trigger.trg</code>	Trigger file	<code>ARBORPATH/app/appname/dbname/</code>
<code>default</code>	Tablespace directory (can be in multiple locations that you define)	(Default location) <code>ARBORPATH/app/appname/default</code>
<code>temp</code>	Tablespace directory (can be in multiple locations that you define)	(Default location) <code>ARBORPATH/app/appname/temp</code>
<code>log</code>	Tablespace directory	<code>ARBORPATH/app/appname/log</code>
<code>metadata</code>	Tablespace directory	<code>ARBORPATH/app/appname/metadata</code>
<code>essn.dat</code>	Aggregate storage data file	<code>ARBORPATH/app/appname/default/</code> <code>ARBORPATH/app/appname/log/</code> <code>ARBORPATH/app/appname/metadata/</code>

- To back up an aggregate storage database:
 - 1 Stop the application.
 - 2 Use the file system to copy the contents of the application directory (*ARBORPATH/app/appname*), excluding the *temp* directory.

Exporting and Importing Partition Definitions

The section applies to block storage and aggregate storage databases.

If you have Database Manager permissions for a partitioned database, you can create backup copies of partition definitions by exporting them. Partition definitions must first be saved to the file system or network as *.xml* files. You can import only partition definition files that have the *.xml* extension.

For instructions on exporting and importing partition definitions, see “Exporting Partition Definitions” and “Importing Partition Definitions” in the *Oracle Essbase Administration Services Online Help*.

Integration Services

- To back up Integration Services:
 - 1 Perform a complete backup of the Oracle Essbase Integration Services catalog repository.
 - 2 **Optional:** Export all models and metaoutlines into XML files.
 - 3 Create and save a list of all source Open Database Connectivity (ODBC) Data Source Names (DSNs) that were set up.
 - 4 Keep a current copy of installed software, along with all property files, such as *ais.cfg*.
- To recover Integration Services:
 - If Integration Services installation files are lost because of hardware failure, you must reinstall Integration Services.
 - If the database containing the catalog is corrupted, you must restore it and then create an ODBC DSN to the catalog and use it to retrieve models and metaoutlines.
 - If the backup catalog database is also corrupted, then, from Oracle Essbase Integration Services Console, create an empty catalog and import each model and metaoutline using XML files.

Essbase Studio

- To back up and restore Essbase Studio components to a previous state:
 - 1 Stop the Oracle Essbase Studio server.

- 2 Perform a complete backup of the Oracle Essbase Studio metadata repository.
- 3 Keep a current copy of installed software and all property files (`server.properties`, `essbase.properties`, and `eas.properties`).

Provider Services

Back up these files and folders:

- `EPM_ORACLE_HOME/products/Essbase/aps/bin/datasources.xml` file—Contains all data source connection information for the various providers.
- `EPM_ORACLE_HOME/products/Essbase/aps/data` folder—Contains all Smart Slice definitions managed centrally by Oracle Hyperion Provider Services
Back up the entire folder, including subfolders.
- `EPM_ORACLE_INSTANCE/products/Essbase/aps/bin/Essbase.properties`

See [Chapter 2, “Common Backup Tasks.”](#)

You can restore the backed up files and folders by returning them to their original locations.

5

Financial Performance Management Applications

In This Chapter

Planning.....	49
Business Rules	50
Disclosure Management.....	50
Financial Close Management.....	51
Financial Management	51
Performance Scorecard	52
Profitability and Cost Management.....	53
Strategic Finance	53

Planning

➤ To enable Planning recovery from a failure:

- 1 Back up related components, as described in [Chapter 2, “Common Backup Tasks.”](#)

Note: Be sure to back up the Planning system database as well as all individual application databases.

Backups of applications and related application databases must include these items:

- The application in Essbase
- The relational database for Planning and Oracle Hyperion Financial Reporting
- Required Planning components

Tip: Rather than back up the entire Windows registry, you can back up only these keys for Planning: HKLM/Software/Oracle* nodes and HKLM/System/CurrentControlSet/Services/Oracle*.

- 2 Back up the Essbase outline files for your applications.
- 3 Back up the full export of Essbase data. See [“Essbase” on page 23](#).
- 4 Back up any calculation scripts and substitution variables associated with Essbase.
- 5 Back up the file system folder that contains Planning shared libraries:

- 32-bit: `EPM_ORACLE_HOME/products/Planning/lib`
 - 64-bit: `EPM_ORACLE_HOME/products/Planning/lib64`
- 6** UNIX: Back up custom scripts, such as startup files associated with Planning.
 - 7** Back up common components in `EPM_ORACLE_HOME/common/planning/11.1.2.0/lib`.
 - 8** Ensure that the backup of `EPM_ORACLE_HOME/products/Planning` directory includes these files, and back them up manually if it does not:
 - `log4j.properties`
 - `essbase.properties`
- To recover after a failure:
- 1** Stop all product and related services. See the *Oracle Hyperion Enterprise Performance Management System Installation and Configuration Guide*.
 - 2** Replace backed up files and directories in the original locations.
 - 3** Restore the Planning databases.
 - 4** Restart all servers and services.

See also [Chapter 4, “Essbase Components.”](#)

Business Rules

- To enable recovery after a failure:
- 1** Back up related components daily to a storage device, as described in [Chapter 2, “Common Backup Tasks,”](#) including databases for the products that you use with Oracle Hyperion Business Rules (such as Planning).
 - 2** Back up the `AdminServices/storage` directory daily.
 - 3** Back up all XML files in `AdminServices/server` daily.
- To recover after a failure:
- 1** Replace the database files with the backup database files on the storage device.
 - 2** Restore the copied Essbase directories, including outline files, to the original location.
 - 3** Populate data in the Essbase database using the backup.
 - 4** Restore the Oracle Hyperion Planning files to the original locations.

Disclosure Management

To enable recovery of Disclosure Management mapping data, back up both the file system (containing taxonomies and documents) and the relational database (containing XBRL mappings and Disclosure Management data). Any taxonomies on the Disclosure Management

server file system must also be backed up. Taxonomy files are in `EPM_ORACLE_HOME/products/DisclosureManagement/DiscManInstance/xbrlfiles`.

- If you are using Oracle Hyperion Smart View for Office, back up any Microsoft Office documents that are used for reports and XBRL mappings.
- If Disclosure Management is integrated with Financial Reporting, also back up reports and any other Financial Reporting artifacts.

Restoring Oracle Hyperion Disclosure Management from a backup requires restoring backed-up taxonomies to their original location, because any reports you have mapped reference these taxonomies in the original file system location.

Financial Close Management

To enable recovery of Financial Close Management data, back up the database and the SOA server. You can perform hot backups or cold backups. See [“Database Backup Types” on page 9](#) and your RDBMS documentation. For instructions on backing up the SOA server, see these chapters in [Oracle Fusion Middleware Administrator's Guide](#):

- Chapter 15, “Introducing Backup and Recovery”
- Chapter 16, “Backing Up Your Environment”
- Chapter 17, “Recovering Your Environment”

Financial Management

Most Financial Management configuration information is in Shared Services Registry, but some is in the Windows registry, in `HKEY_LOCAL_MACHINE/SOFTWARE/Oracle Solutions/Hyperion Financial Management`. Distributed Component Object Model (DCOM) security information is associated with `HFMServer.exe` and `HsvDataSource.exe`. Because backing up and restoring this information is difficult, use the following procedure on every application and Web server to back up Financial Management.

► To enable recovery of Financial Management:

- 1 **Perform a full database backup once per cycle:**
 - a. Stop Financial Management Web Services and IIS.
 - b. Stop these related services:
 - `HsxService.exe`
 - `DMEListener.exe`
 - `HFMWebServiceManager.exe`
 - c. Stop these related processes:
 - `HsxServer.exe`
 - `HsvDatasource.exe`

- CASecurity.exe

- 2 **Back up the Windows registry export for** `HKEY_LOCAL_MACHINE/SOFTWARE/Oracle Solutions/Hyperion Financial Management`.
- 3 **Back up the Shared Services Registry.**
- 4 **Back up any customized style sheets.**

Note: You must also back up Oracle Hyperion Shared Services, and you might need to back up Reporting and Analysis for related content.

➤ To recover from an application server or Web server failure:

- 1 **Reinstall and configure Financial Management on the failed application or Web server.**
- 2 **Stop all Financial Management processes and services on the newly configured server.**
- 3 **Restore the backed-up files to their original locations.**
- 4 **Restart the services.**

➤ To recover from a database server failure:

- 1 **Stop all Financial Management processes and services on all application and Web servers.**
- 2 **Restore the database from the last full backup, applying transaction logs as needed.**

If you restore a Oracle Hyperion Financial Management, database to a machine other than the machine where the database was created and the application server names have changed, you must delete these tables from the database:

- HSX_Cluster_Cont_info
- HSX_Cluster_Controllers
- HSX_Cluster_Info
- HSX_Cluster_Servers

If you delete the tables, must rerun Oracle Hyperion Enterprise Performance Management System Configurator to recreate cluster definitions.

- 3 **Restart the database.**
- 4 **Restart the application and Web servers.**

Performance Scorecard

➤ To enable recovery from a failure:

- 1 **Regularly back up these items:**
 - Related components as described in [Chapter 2, “Common Backup Tasks.”](#)

- The directory containing attachments (`EPM_ORACLE_INSTANCE/HPS/hpsfiles/attachments` by default)
 - The directory containing notes (`EPM_ORACLE_INSTANCE/HPS/hpsfiles/notes` by default)
 - `HPSConfig.properties` and `AlerterConfig.properties` in `EPM_ORACLE_INSTANCE/HPS/hpsfiles/config`
- 2 If you generated an Essbase database of application data, back up the database as described in [Chapter 4, “Essbase Components.”](#)
 - 3 If you installed the ETL Import Export Utility, back up these directories:
 - `EPM_ORACLE_INSTANCE/HPS/hpsfiles/tools/config`
 - `EPM_ORACLE_INSTANCE/HPS/hpsfiles/tools/bin`
- To recover from a failure, replace the copied directories and files in their original locations and restore the database.

Profitability and Cost Management

- To enable Profitability and Cost Management recovery from a failure:
- 1 Back up related components as described in [Chapter 2, “Common Backup Tasks.”](#)
- Note:** If you use Profitability and Cost Management with Oracle Hyperion Financial Reporting or Oracle Hyperion Web Analysis, you must also back up those products.
- 2 Back up the Oracle Hyperion Profitability and Cost Management import staging area and the operational data store.
- Use the backup tools for your relational database. This could include using scripting or scheduler scripts.
- 3 Back up Oracle Essbase applications, databases, calculation scripts, and data filters.
- See [Chapter 4, “Essbase Components,”](#) and the *Oracle Essbase Database Administrator's Guide*.
- To recover from a failure, restore the backed-up components to their original locations and restore the database.

Strategic Finance

- To enable Strategic Finance recovery from a failure:
- Back up related components as described in [Chapter 2, “Common Backup Tasks.”](#)

- Record the optional RDBMS connection information.
- Back up the application data folder (*EPM_ORACLE_HOME/products/hsf/hsfdata* by default).
- Copy customization files such as *.coa* files, *currdata.dat*, *consdata.dat*, and *convert.idx* to another location or to a storage device.
- If you use custom templates, back up the contents of the server program directory, including *.coa*, *.idx*, *.dat*, *.txt*, *.xml*, *.drs*, *.alt*, and *.alc* files.
- Back up Windows registry settings on the Strategic Finance server. See [“Backing Up Windows Registry Settings” on page 16](#).

Note: Use of the “back up open files” option of standard backup products is recommended, in case Strategic Finance is holding files open when the backup goes through the application data folder. If the open files are not backed up, the backup image may not be fully consistent.

➤ To recover Strategic Finance from a failure:

- 1 Reinstall Oracle Hyperion Strategic Finance Server.
- 2 Copy the backed-up files to the new installation directory.
- 3 Restore any other components that you backed up.
- 4 Reestablish the connection for data export from Oracle Hyperion Strategic Finance, to the RDBMS.
- 5 Restart Oracle Hyperion Strategic Finance Server.

6

Reporting and Analysis

In This Chapter

Backing Up the Reporting and Analysis File System.....	55
Reporting and Analysis Services Suspension	56
Restoring Reporting and Analysis	57
Dashboard Development Services	57
Financial Reporting	58
Production Reporting	58

Note: In general, you should back up Reporting and Analysis components along with EPM Workspace. See “[EPM Workspace and Shared Services](#)” on page 19.

Backing Up the Reporting and Analysis File System

► To back up the file system:

1 After installing Reporting and Analysis, back up these directories:

- `EPM_ORACLE_HOME/products/biplus`
- `EPM_ORACLE_INSTANCE/config/ReportingAnalysis`
- `EPM_ORACLE_INSTANCE/ReportingAnalysis`
- `EPM_ORACLE_INSTANCE/bin/ReportingAnalysis`
- `EPM_ORACLE_INSTANCE/products/biplus`
- Any directories that you specified for Reporting and Analysis files if you did not accept the defaults during installation and configuration.

2 Perform weekly full or daily incremental backups of these items:

- (Windows only) Templates, styles, palettes, and components in `EPM_ORACLE_HOME/products/biplus/DDS`
- Custom development resources, such as dashboards and scripts
- Any custom components, scripts, and version-controlled data
- `EPM_ORACLE_INSTANCE/diagnostics/logs/ReportingAnalysis`

- For EPM Workspace modules, Oracle Hyperion Enterprise Performance Management Workspace search index files in `EPM_ORACLE_HOME/common/raframeworkrt/11.1.2.0/wsearch`
- `EPM_ORACLE_HOME/common/raframeworkrt/11.1.2.0/wsearch`
- Repository Manager location

Note: This location (`EPM_ORACLE_INSTANCE/ReportingAnalysis/data/RM1` by default) is set during Reporting and Analysis configuration.

3 Back up ANDALE fonts (ANDALE*.ttf) in C:/Windows/Fonts (Windows) or `EPM_ORACLE_HOME/products/biplus/fonts` (UNIX).

In a UNIX environment, Oracle recommends backing up the entire folder, because it contains `fonts.dir` in addition to `ANDALE*.ttf` files.

Reporting and Analysis Services Suspension

Note: The following information pertains to services that are in the Oracle Hyperion Shared Services Registry.

Rather than shut down services before performing a backup, you can suspend services by putting them in maintenance mode. This process initially includes running a SQL statement to insert a row in the `v8_service_mode` table in the Oracle Hyperion Reporting and Analysis repository schema with the values of `v8_service_mode.name="MAINTENANCE"` and `v8_service_mode.value = 1`.

Delay the start time by increasing the default value of `v8_service_mode.start_delay=minutes`. For example, if `setv8_service_mode.value=1` and `v8_service_mode.start_delay=30`, services reject requests after 30 minutes.

While services are suspended:

- Users cannot perform actions carried out by Oracle Hyperion Reporting and Analysis Framework services, such as browse repository content, work with repository items, and execute jobs.
- Read/write requests to the Reporting and Analysis Framework services database are not processed.
- Oracle Hyperion Reporting and Analysis Framework services background activities that result in database updates, such as repository garbage collection, are put on hold.
- Event Service activity is put on hold.

Service log messages indicate that the service is in maintenance mode. Messages are also logged when maintenance mode is turned off.

To turn off maintenance mode after the backup, change the `.v8_service_mode.value` setting to 0.

Restoring Reporting and Analysis

➤ To restore Reporting and Analysis:

- 1 Restore the components that you backed up.
- 2 Restore **ANDALE*.TTF fonts** to (C:/Windows/Fonts) **for Windows** or *EPM_ORACLE_HOME/products/biplus/fonts* **for UNIX**.
- 3 Recover the database by stopping all related services, restoring the database using the same path from which you backed it up, and restarting the services.

Dashboard Development Services

➤ To enable Dashboard Development Services recovery from a failure, back up these components:

- Databases used by Dashboard Development Services dashboards
- Templates, styles, palettes, and components in *EPM_ORACLE_HOME/products/biplus/DDS*
- Custom development resources, such as dashboards, scripts, and version-controlled data

See [Chapter 2, “Common Backup Tasks.”](#)

➤ To recover from a failure:

- 1 Replace all backed-up components in their original locations.
- 2 If you did not back up and restore the Windows registry entries for the Oracle Hyperion Dashboard Development Services ActiveX components, register them by running these commands:

- `regsvr32 EPM_ORACLE_HOME/products/biplus/bin/QIQZip.dll`
- `regsvr32 EPM_ORACLE_HOME/products/biplus/bin/DDSUtil.dll`
- `regsvr32 EPM_ORACLE_HOME/products/biplus/bin/DDSFW.dll`
- `regsvr32 EPM_ORACLE_HOME/products/biplus/bin/DDSHelper.dll`
- `regsvr32 EPM_ORACLE_HOME/products/biplus/bin/DDSListBar.ocx`
- `regsvr32 EPM_ORACLE_HOME/products/biplus/bin/Srcvw3.dll`
- `regsvr32 EPM_ORACLE_HOME/products/biplus/bin/MBSplit.ocx`
- `regsvr32 EPM_ORACLE_HOME/products/biplus/bin/UniBox10.ocx`
- `regsvr32 EPM_ORACLE_HOME/products/biplus/bin/UniBoxVB12.ocx`
- `regsvr32 EPM_ORACLE_HOME/products/biplus/bin/UniBox210.ocx`
- `EPM_ORACLE_HOME/products/biplus/bin/DDSDebugProxy.exe`
- `EPM_ORACLE_HOME/products/biplus/bin/DDSDebugSrv.exe`

Financial Reporting

- To enable recovery of Financial Reporting, back up related components as described in [Chapter 2, “Common Backup Tasks.”](#)
- To restore Financial Reporting, replace all backed up components.

Production Reporting

- To enable Production Reporting recovery:
 - 1 Back up these Microsoft Windows directories:**
 - %windir%/sqr.ini
 - %windir%/sqr64.ini
 - %windir%/libsti.ini
 - 2 Back up these directories in *EPM_ORACLE_HOME*/products/biplus:**
 - bin/SQR/...
 - common/SQR/...
- To recover Production Reporting after a failure, replace the backed-up components in their original locations and restore the database.

7

Data Management

In This Chapter

Data Relationship Management.....	59
FDM	60
ERP Integrator	60

Data Relationship Management

Data Relationship Management uses separate databases and schemas for each application that you create.

► To enable Data Relationship Management recovery from a failure:

- 1 **Back up related components and application databases as described in [Chapter 2, “Common Backup Tasks.”](#)**
- 2 **Regularly back up these files in `EPM_ORACLE_HOME/products/DataRelationshipManagement/server/config` to a storage device:**
 - `drm-config.xml`—Connection information for all Data Relationship Management applications that are hosted on the machine
 - `drm-helper.bin`—Database authentication information for each Data Relationship Management application that is hosted on the machine.

This file can be used only on the machine on which it was created. Using Data Relationship Management Console, you can reproduce `drm-helper.bin` by reentering the database connection passwords for each application and then saving the configuration. You can reproduce `drm-helper.bin` only with Data Relationship Management Console.
- 3 **If you have configured customized logging, back up `drm-log4net.xml`, in `MIDDLEWARE_HOME/EPMSysm11R1/products/DataRelationshipManagement/server/config`.**
- 4 **Back up `EPM_ORACLE_HOME/products/DataRelationshipManagement/client/drm-client-application/Web.Config` whenever `Web.Config` is edited.**
- 5 **Back up scripts for the Data Relationship Management Batch Client that are used to run automated processes. The location of these files depends on the computer where the Batch Client program is run.**

- 6 Back up XML files created by the Oracle Hyperion Data Relationship Management Migration Utility (for archival purposes). The location of these files depends on the computer where the Migration Utility is run.
- To recover after a failure:
 - 1 Restore the copied database and configuration files to their original locations.
 - 2 Reenter the passwords for the database in the configuration file.

FDM

Oracle Hyperion Financial Data Quality Management uses separate databases and schemas for each application that you create.

- To enable recovery after a crash, perform these tasks regularly:
 - Back up the databases that you use, as described in the database vendor documentation.
 - Back up the entire application folder structure (Inbox, Outbox, Data, and so forth) to a storage device.
- To recover after a failure, restore the directory to its original location and restore the database as described in the database vendor documentation.

ERP Integrator

- To enable ERP Integrator recovery after a crash, regularly back up the database schema that stores the mapping tables and data staging tables.
- To recover after a failure, restore the directory to its original location and restore the database as described in the database vendor documentation.

Index

A

archiving Essbase files, [41](#)

B

backup preliminaries, [13](#)

backup types

database, [9](#)

file system, [10](#)

BEGINARCHIVE command (Essbase), [41](#)

Business Rules

backup, [50](#)

recovery, [50](#)

C

Calculation Manager backup and recovery, [22](#)

D

Dashboard Development Services

backup, [57](#)

recovery, [57](#)

Data Relationship Management

backup, [59](#)

recovery, [60](#)

database backup

common tasks, [13](#)

logical, [10](#)

physical, [9](#)

with Lifecycle Management, [10](#)

databases, Shared Services Registry, [13](#)

Disclosure Management, [50](#)

disk volumes, backing up Essbase data on, [40](#)

documentation, [7](#)

E

ENDARCHIVE command (Essbase), [42](#)

EPM Workspace

file system backup, [19](#)

recovery, [20](#)

suspending services, [56](#)

ERP Integrator

backup, [60](#)

recovery, [60](#)

Essbase

archive replay data, removing, [38](#)

archiving data, [41](#)

backing up and restoring data files, [39](#)

backing up files during runtime, [40](#)

backup (manual procedures), [39](#)

backup and recovery overview, [23](#)

BEGINARCHIVE command, [41](#)

binary data export and import, [42](#)

block storage database

backup and recovery, [24](#)

backup and restore feature, [25](#)

recovery sequence, [24](#)

restoring, [30](#)

transaction logging and replay, [32](#)

calculation scripts, clearing after export, [45](#)

data corruption, avoiding, [41](#)

data export, [42](#)

database

aggregate storage, [46](#)

backup caution, [41](#)

large files, [44](#)

resolving corruption, [45](#)

restoring, [42](#)

dirty status after reloads, [44](#)

disk volumes, [31](#)

environment variables, preserving, [46](#)

essential files, [40](#)

exported data reloads, [42](#)

exporting data in parallel, [44](#)

file system backup, [40](#)

LRO links, maintaining, [45](#)

PAREXPORT command, [43](#)
 partitioned databases
 backup and recovery, [32](#)
 using transaction logging and replay, [39](#)
 partitions, backing up, [47](#)
 putting a database in read-only mode, [41](#)
 recalculating data after exporting, [44](#)
 restoring manually backed up files, [31](#)
 retrieving archive file information, [29](#)
 transaction log
 configuring security for replay, [37](#)
 replaying, [37](#)
 using with partitioned databases, [39](#)
 viewing, [35](#)
 transaction log store removal, [38](#)
 transaction logging, enabling, [33](#)
 transaction replay, configuring, [34](#)
 Unicode and non-Unicode applications, [31](#)

Essbase databases

 exporting, [43](#)

Essbase operations (archiving, stopping, cancelling),
[41](#)

Essbase Studio backup and recovery, [47](#)

EXPORT command (Essbase), [44](#)

exported data, reloading (Essbase), [42](#)

F

FDM

 backup, [60](#)

 recovery, [60](#)

file system backup

 overview, [14](#)

 types, [10](#)

Financial Close Management, [51](#)

Financial Management

 backup, [51](#)

 recovery

 application server or Web server failure, [52](#)

 database server failure, [52](#)

Financial Reporting

 backup, [58](#)

 recovery, [58](#)

I

installation documentation, [7](#)

Integration Services

 backup, [47](#)

 recovery, [47](#)

L

Lifecycle Management, backup with, [10](#)

M

MaxL

 data export, [43](#)

 data import, [44](#)

 switching to read-only mode, [41](#)

 switching to read/write mode, [42](#)

O

operating system settings backup, [16](#)

OS. *See* operating system

P

PAREXPORT command (Essbase), [44](#)

partitions (Essbase), backing up, [47](#)

Performance Management Architect

 backup, [21](#)

 recovery, [21](#)

Performance Scorecard

 backup, [52](#)

 recovery, [53](#)

Planning

 backup, [49](#)

 recovery, [50](#)

platforms (Essbase applications), porting, [42](#)

Production Reporting

 backup, [58](#)

 recovery, [58](#)

Profitability and Cost Management

 backup, [53](#)

 recovery, [53](#)

Provider Services backup and recovery, [48](#)

R

recovery sequence, [11](#)

regedit, component backup with, [16](#)

Reporting and Analysis

 file system backup, [55](#)

 recovery, [57](#)

 suspending, [56](#)

S

services, suspending for EPM Workspace and

Reporting and Analysis, [56](#)

Shared Services

file system backup, [19](#)

Smart View

backup, [22](#)

recovery, [22](#)

Strategic Finance

backup, [53](#)

recovery, [54](#)

system variable backup, [17](#)

W

Windows registry settings backup, [16](#)

