Oracle® Collaboration Suite

Backup and Recovery

Release 2 (9.0.4)

Part No. B15613-03

April 2005

About this document

The purpose of this document is to discuss the general methodology for backup and recovery of the Oracle Collaboration Suite. For information on backup and recovery of individual components of the Oracle Collaboration Suite,

> **See Also:**
>
> - *Oracle Wireless Administrator's Guide*
>
> - *Oracle Web Conferencing Administrator's Guide*
>
> - *Oracle Files Administrator's Guide*
>
> - *Oracle Email Administrator's Guide*
>
> - *Oracle Calendar Administrator's Guide*
>
> - *Oracle Ultra Search Administrator's Guide*
>
> - *Oracle Voicemail and Fax Administrator's Guide*

Acknowledgements

Roza Leyderman was the primary author for this document, but it could not exist without the skills and dedication of the following individuals: Simon Azriel, Y.C. Cheung, Soulaiman Htite, Shuvayu Kankulal, William Kehoe, Jerald Jensen, Sandra Lee, Francois Perrault, Sylvester Rajasekaran, Jean-Marc Robillard, Sudip Roy, Padmanabhan Sadagopan, and Ricardo Rivera.

Contents

This document contains the following topics:

- Oracle Collaboration Suite Basics

- Oracle Collaboration Suite Backup and Recovery Strategy

- Understanding Database Backup and Recovery

- Understanding the Oracle Collaboration Suite Backup and Recovery Tool

- Understanding Dynamic Plug-In Input Files

- Understanding Calendar Backup and Recovery

- Oracle Collaboration Suite Backup and Recovery Procedures

- Documentation Accessibility

ORACLE®

1 Oracle Collaboration Suite Basics

The Oracle Collaboration Suite offers the user a number of integrated software services that can be deployed in different configurations. Depending on the configuration choice, an Oracle Collaboration Suite instance has varying properties of availability, scalability, application service component deployment, flexibility for growth, and failure coupling.

Oracle Collaboration Suite uses the Oracle9*i* Application Server and the Oracle9*i* Database to provide services that enable communication and collaboration between users. Figure 1 illustrates these options:

- Users can send emails, receive voicemails and faxes, organize their appointments, share documents, search for information and conduct online meetings.

- Users can interact with these services over the web, by fax, using client applications such as Microsoft Outlook, by voice, or over wireless networks using phones and PDAs.

Figure 1   Oracle Collaboration Suite Components
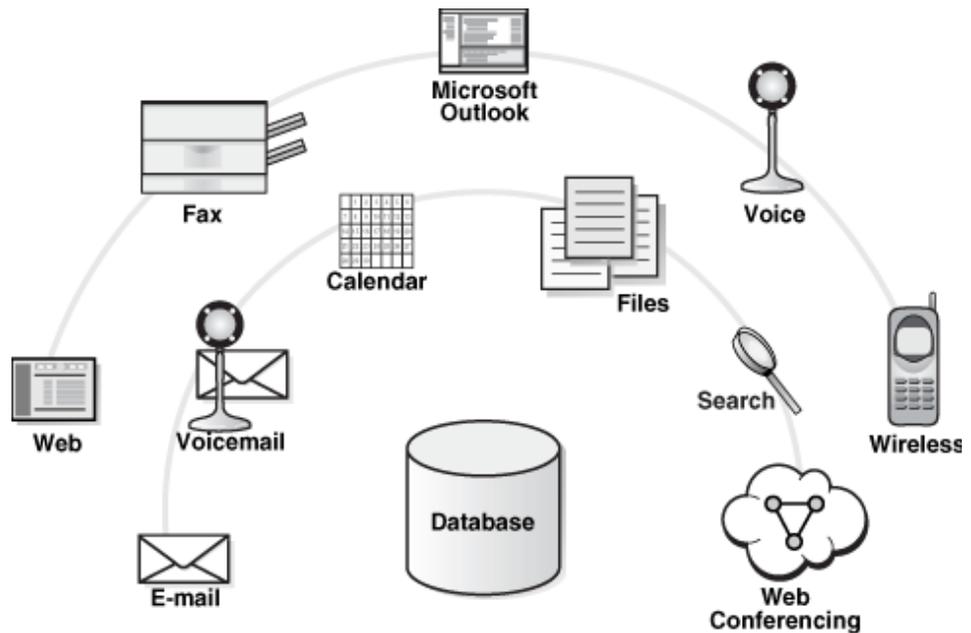
> **See Also:** *Oracle Collaboration Suite Concepts Guide* and the *Oracle Collaboration Suite Deployment Guide* for a discussion of Oracle Collaboration Suite deployment options and their characteristics.
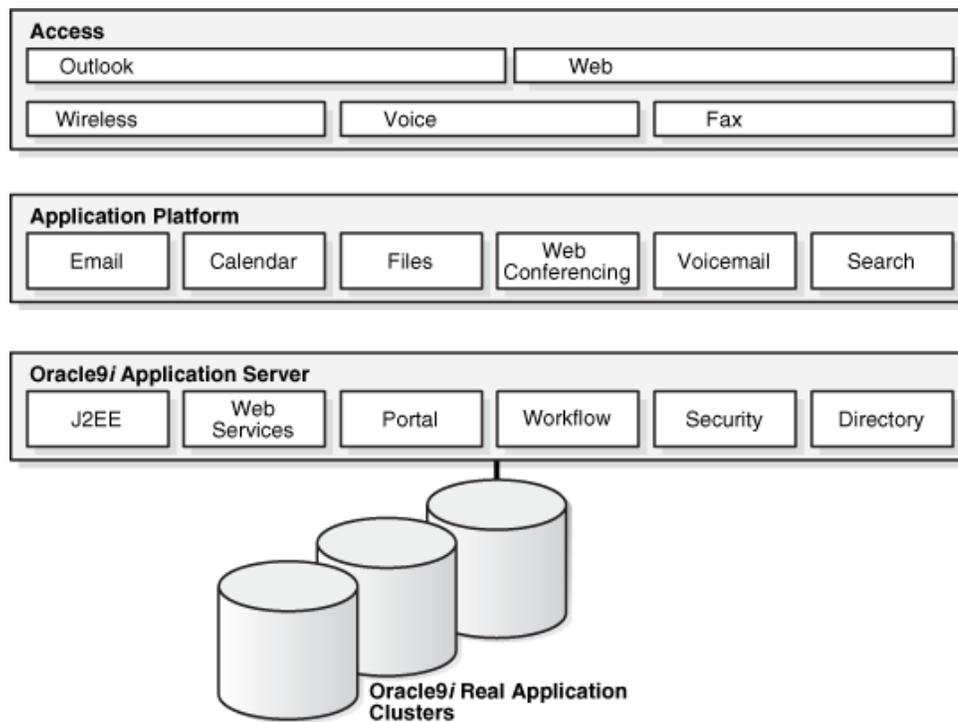
1.1 Oracle Collaboration Suite Architecture

Looking at the Oracle Collaboration Suitesuite from a high architectural level, we can consider it to be composed of three main layers:

- The **Infostore**, or data tier, is built on the Oracle9*i* Database and contains Files and Email databases.

- The **Infrastructure** tier is built on Oracle9*i* Application Server, and comprises a common set of services used by the applications. These include Java execution (J2EE), Web Services, Portal, Workflow, Security and Directory.

- The **Middle** tier includes the Email, Calendar, Files, Web Conferencing, Voicemail and Search applications themselves. These can be accessed through a wide range of channels, such as Wireless, Voice, Fax, Web and Outlook.

The actual deployment architecture is very flexible, and there are several options regarding how these layers are placed into physical server hardware and the ways that the required security, availability, scalability and ease of management is implemented. Figure 2 shows an example of Oracle Collaboration Suite architecture.

Figure 2   Sample Oracle Collaboration Suite Architecture

1.2 Workload Distribution and Security

While all of the three tiers of Oracle Collaboration Suite could be placed on a single node, this is very unlikely to meet your security and availability requirements in any but a few very small system scenarios.

Distribution of the layers should always be considered. The nature of the middle tier, infrastructure and infostore workloads differ greatly:

- While the middle tier uses CPU and memory intensively with little disk I/O, the infrastructure and infostore are very intensive in disk I/O.

- While the infostore disk I/O consists of both reads and writes, the infrastructure disk is primarily used in I/O reads.

To obtain optimum resource utilization from a particular machine and software configuration, you should not to mix different workloads on a single machine. For this reason, architectures, especially for larger systems, typically feature the distribution of these tiers onto different machines. In Oracle Collaboration Suite, middle tier resource demands scale at a different rate than the infrastructure and infostore. This adds further justification for a distributed architecture that allows the infostore and middle tier to be scaled independently.

1.3 Details of Oracle Collaboration Suite Components and Protocols

Figure 3 provides a somewhat simplified detail of the three layers of Oracle Collaboration Suite: Middle Tier, Infostore and Infrastructure:

Figure 3   Oracle Collaboration Suite Tiers
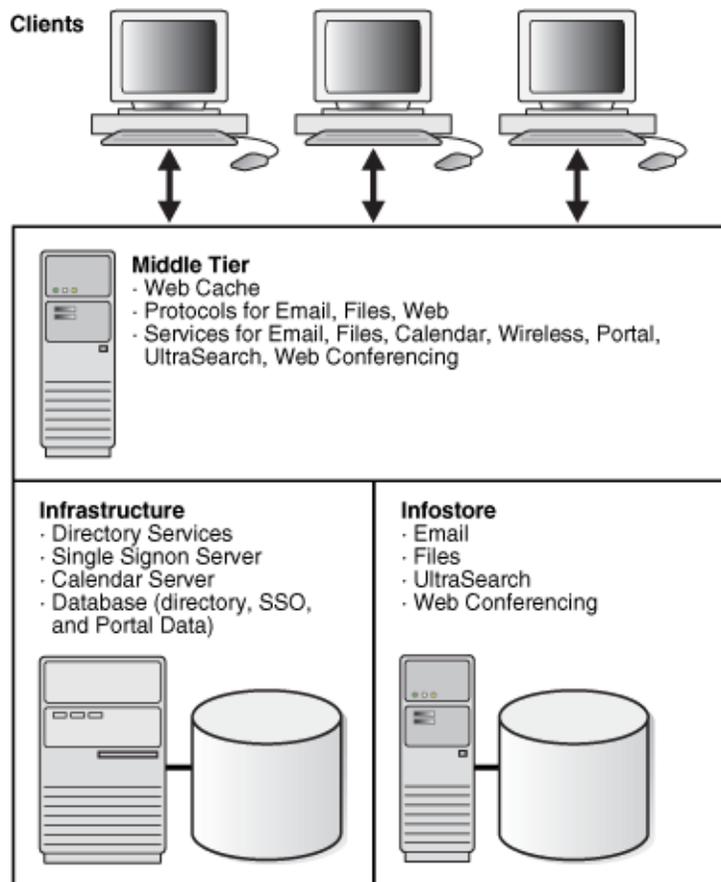
1.3.1 Middle Tier

The Middle tier consists of the following services:

- Email Protocols (SMTP, POP3, IMAP4)

- Files Protocols (FTP, SMB, NFS, AFP, WebDav)

- Web Protocols (HTTP, HTTP/S)

- Email Services (Webmail/HTTP)

- Files Services (Files/HTTP)

- Calendar Services (Webcal/HTTP, SyncML/HTTP, Calendar Server)

- Wireless Services (Wireless/HTTP)

- Portal Services (Portal/HTTP)

- UltraSearch Services

- Webcache

1.3.2 Infrastructure Tier

The Infrastructure includes the following:

- Directory Services (LDAP, DAS/HTTP)

- Single Sign On Server (SSO/HTTP)

- Infrastructure database containing Directory, SSO and Portal data

1.3.3 Infostore Tier

The Infostore includes the following databases:

- Email

- Files

- UltraSearch

2 Oracle Collaboration Suite Backup and Recovery Strategy

This section provides an introduction to backup and recovery concepts, an overview of Oracle's backup and recovery strategy in an enterprise environment, and assumptions and restrictions necessary to implementing this strategy.

2.1 Basics of Backup and Recovery

Because all organizations need to protect themselves from potential disaster resulting from data loss, backup and recovery is one of the most important aspects of administration.

Your Oracle Collaboration Suite environment is the framework within which you perform backup and recovery, and contains the following tiers, as previously discussed in Section 1.3 and illustrated in Figure 3, "Oracle Collaboration Suite Tiers": an infostore installation, an infrastructure installation, and a middle tier installation.

These installations contain interdependent configuration information, applications, and data. During normal operation, the application server automatically synchronizes this information. However, in the event of system failure or data loss, the administrator has to restore the application server to a consistent state.

For this reason, it is important to visualize the Oracle Collaboration Suite environment as a single entity when performing backup and recovery, instead of approaching it as a set of independent installations. As a result, you must back up data across all installations at the same point in time. If you were backing up the infrastructure on Mondays, the infostore on Tuesdays and the middle tier installation on Wednesdays, in the event of data loss you would only be able to

restore your separate tiers of the Oracle Collaboration Suite to the state they had on the days when they were last saved. This would create problems in the application server. If you backup critical data from all tiers at the same time, you can restore and recover all tiers to a consistent state.

The backup and recovery strategies and procedures in this document involve backing up the entire Oracle Collaboration Suite environment as a whole and restoring it so that its state remains consistent.

2.2 Oracle Collaboration Suite Backup and Recovery Roadmap

The overall backup strategy should be comprised of a cold backup and partial online backups.

You should perform an initial complete **cold backup**, which includes everything necessary to restore your initial installation of your Oracle Collaboration Suite environment:

- Back up the middle tier Oracle home

- Back up the infrastructure Oracle home

- Back up the infostore Oracle home

- Back up Calendar and its associated files

You should also perform regular **partial online backups** of your Oracle Collaboration Suite environment, which involves saving the configuration information across your entire Oracle Collaboration Suite environment at the same point in time:

- Back up the configuration files in the middle tier Oracle home

- Back up the configuration files in the infrastructure Oracle home

- Back up configuration files in the infostore Oracle home

- Perform an online backup of the infrastructure

- Perform an online backup of the infostore

Restore and recovery procedures for **data loss**, **host failure**, or **media failure** enable you to recover from failures that involve actual data loss. Depending on the type of loss, they can involve a variety of steps. In all cases, care must be taken to ensure that state is consistent across all installations:

- Restore Oracle static binaries or libraries from a complete cold backup

- Restore configuration files from the most recent partial online backup

- Restore and recover the infrastructure to its latest state

- Restore and recover the infostore to its latest state

Recovery strategies for **process or system outages** and **crashes** involve restarting processes that have stopped or failed. They do not involve data recovery.

More specifically, Oracle recommends that you use one of the following general strategies to implement backup and recovery within your organization. Both strategies have the following common characteristics:

- These strategies use complete recovery for the infrastructure and infostore. Specifically, they restore the backup and then apply all online and archived

redo logs generated after the restored backup. This recovers the database to the state it had at the time of the loss.

- These strategies use same-point-in-time recovery of the middle tier, infrastructure, and infostore. Regardless of where the loss occurred, the middle tier, the infrastructure and the infostore are always restored together so they are synchronized as they were at the time of the most recent backup.

2.2.1 Oracle Collaboration Suite Backup and Recovery Using the Oracle Collaboration Suite Backup and Recovery Tool and Recovery Manager (RMAN)

Oracle developed the Oracle Collaboration Suite Backup and Recovery Tool for Oracle Collaboration Suite installations. In conjunction with RMAN, its automated scripts enable a quick deployment of the Oracle Collaboration Suite backup and recovery strategy. This entire strategy can be summarized in the following steps:

1. Use the Oracle Collaboration Suite Backup and Recovery Tool for backing up and restoring the middle tier and the infrastructure database.

2. Use RMAN to backup and recover the infostore.

3. Use Oracle Collaboration Suite Calendar backup and recovery utilities.

2.2.2 Oracle Collaboration Suite Backup and Recovery Using Only the Recovery Manager (RMAN) and Other Customized Scripts

If your organization is using customized backup and recovery operations already, you may not wish to use the Oracle Collaboration Suite Backup and Recovery Tool as part of your Oracle Collaboration Suite backup and recovery strategy. The general steps would then be as follows:

1. Use RMAN and/or customized scripts to back up and restore the infrastructure and infostore databases.

2. Use customized scripts to backup and restore the middle tier and its components.

3. Use Oracle Collaboration Suite Calendar backup and recovery utilities.

2.3 Assumptions and Restrictions for all Oracle Collaboration Suite Backup and Recovery Operations

Prerequisites to suite-level backup and recovery include:

- Oracle Collaboration Suite support is limited to the 9.0.4.2 release.

- These installation types are supported:
  - J2EE and Web Cache
  - Portal and Wireless
  - Infrastructure
  - Infostore

- All operating system platforms that are certified for Oracle Collaboration Suite are supported.

- Each host must have a Perl installation of version 5.0 or above.

- The infrastructure must be a single instance database. The procedures in this document do not support using Real Application Clusters (RAC).

- When restoring the Oracle Collaboration Suite, you should restore to the same host. When this is not possible, you can restore to a new host provided you first initialize it with the same system configuration as the original host, such as hostname, IP address, user names, directory paths, and operating system levels.

- You should turn on database archive logging since point-in-time recovery is a requirement.

- Before running the Oracle Collaboration Suite Backup and Recovery Tool:

  - Log in as the user that installed Oracle Collaboration Suite.

  - Make sure the ORACLE_HOME environment variable is set.

  - If you are performing a database backup, make sure the ORACLE_SID environment variable is set.

  - Change directory to the directory that contains the installed Oracle Collaboration Suite Backup and Recovery Tool.

3 Understanding Database Backup and Recovery

The Oracle Collaboration Suite environment includes the infostore tier, an Oracle9*i* Release 1 (9.0.1) Enterprise Edition database. Performing backup and recovery on Oracle Collaboration Suite includes performing backup and recovery of that database. It is therefore important to understand database backup and recovery. In particular, the following topics apply to Oracle Collaboration Suite backup and recovery:

- Using ARCHIVELOG mode, as discussed in Section 7.4.1, "Enabling ARCHIVELOG Mode"

- Performing cold database backups, as discussed in Section 7.3.1, "Performing Cold Database Backups"

- Performing online database backups, as discussed in Section 7.3.2, "Performing Online Database Backups"

- Using the RMAN backup and recovery utility

   See also: The following books in the Oracle 9i Release 1 (9.0.1) documentation set if you are not experienced with database backup and recovery.

   - *Backup and Recovery Concepts*, Part Number A90133-02

   - *Recovery Manager User's Guide*, Part Number A90135-01

   - *Recovery Manager Reference*, Part Number A90136-02

   You can find these volumes in the database document library, at:

   http://www.oracle.com/technology/documentation

3.1 Types of Database Backup

Since a database contains a wide variety of data, database administrators must decide what information they should copy when developing a backup and

recovery strategy. The basic principle is to prioritize data depending on its importance and the degree to which it changes. For example, archive logs do not change, but they are crucial for recovering the database, so multiple copies should be maintained whenever possible. Expense account tables, however, are constantly updated by users. Therefore, this tablespace should be backed up frequently to prevent having to apply large chunks of redo data during recovery.

Backups can be combined in a variety of ways, such as combining weekly whole database backups (to ensure a relatively current copy of original database information) with daily backups of the most accessed tablespaces. Another approach is to multiplex control file and archived redo logs as an additional safeguard. The following list describes the basic backup types:

- **Online Database Backup** An online backup or also known as an open backup, is a backup in which all read-write datafiles and control files have not been checkpointed with respect to the same log sequence number (SCN). For example, one read-write datafile header may contain an SCN of 100 while other read-write datafile headers contain an SCN of 95 or 90. Oracle cannot open the database until all of these header SCNs are consistent, or until all changes recorded in the online redo logs have been saved to the datafiles on disk. For databases that must be running non-stop, you have no choice but to perform online backups of a the entire database in ARCHIVELOG mode.

- **Offline Database Backup** In this backup, all datafiles and control files are consistent to the same point in time (or the same SCN). The only tablespaces in a consistent backup that are allowed to have older SCNs are read-only and offline-normal tablespaces, which are consistent with the other datafiles in the backup. This type of backup allows you to open the set of files created by the backup without applying redo logs because the data is already consistent. The only way to perform this type of backup is to shut down the database cleanly and make the backup while the database is closed. A consistent whole database backup is the only valid backup option for databases running in NOARCHIVELOG mode.

- **Whole Database Backup** The most common type of backup, the whole database backup contains the control file along with all database files that belong to that database. If the database is operating in ARCHIVELOG mode, you also has the option of backing up different parts of the database over a period of time.

- **Tablespace Backups** A tablespace backup is a subset of the database. Tablespace backups are only valid if the database is operating in ARCHIVELOG mode. The only time a tablespace backup is valid for a database running in NOARCHIVELOG mode is when that tablespace is read-only or offline-normal.

- **Datafile Backups** A datafile backup contains a single datafile. This approach is not as common as tablespace backups, and is only valid for databases that are in ARCHIVELOG mode. The only time a datafile backup is valid for a database running in NOARCHIVELOG mode is if that datafile is the only file in a tablespace.

- **Control File Backups** A control file backup saves the database's control file. If the database is open, you can create a valid backup through the Recovery Manager (RMAN) or by issuing the following SQL statement:

```
ALTER DATABASE BACKUP CONTROLFILE TO LOCATION
```

- **Archived Redo Log Backups** Archived redo logs are necessary for successful media recovery. Depending on the disk space available and the number of transactions executed on the database, you should keep the maximum number of days of archive logs on disk, and you should back them up regularly to ensure a more complete recovery.

- **Configuration Files Backup** Configuration files may be of `spfile` or `init.ora`, password file, `tnsnames.ora`, and `sqlnet.ora`. Since these files do not change often, they require a less frequent backup schedule.

3.2 Types of Database Recovery

There are three basic types of recovery: instance recovery, crash recovery, and media recovery. Oracle performs both instance and crash recovery automatically at instance startup, but media recovery requires additional steps.

- An **instance recovery** is only possible in an Oracle Real Applications Cluster configuration; it occurs in an open database when one instance discovers that another instance has crashed. A surviving instance automatically uses the redo log to recover the committed data in the database buffers that were lost when the instance failed. Oracle also undoes any in-progress transactions on the failed instance and clears any locks held by the crashed instance after recovery is complete.

- A **crash recovery** occurs when either a single-instance database or all instances of a multi-instance database crash. An instance must open the database and then execute recovery operations. In general, the first instance to open the database after a crash or `SHUTDOWN ABORT` automatically performs crash recovery.

- A **media recovery** is executed on the user's command, usually in response to media failure. Online or archived redo logs can be used to make a restored backup current, or to update it to a specific point in time. Media recovery can restore the whole database, a tablespace or a datafile, and recover them to a specified time.

A restored backup can always be used to perform the recovery. There are two principal types of media recovery: complete and incomplete recovery. **Complete recovery** involves using redo log data along with a backup of a database, tablespace, or datafile, to apply every change that took place after the most recent backup, and to ensure that the recovery is to the most current point in time. Typically, media recovery is performed after a media failure damages datafiles or the control file. If you do not recover the database to the most current time, you must specify how far to recover in one of the following ways:

- Tablespace point-in-time recovery (TSPITR) recovers one or more tablespaces to a point-in-time that is different from the rest of the database.

- Time-based recovery, also called point-in-time recovery (PITR), recovers the data up to a specified point in time.

- Cancel-based recovery which recovers data until the `CANCEL` command.

- Change-based recovery, or log sequence recovery, recovers data up to a specified SCN in the redo record if using O/S commands.

If using RMAN, log sequence recovery recovers up to a specified log sequence number. When performing an **incomplete recovery**, the user must reset the

online redo logs when opening the database. The new version of the reset database is called a new incarnation. Opening the database with the `RESETLOGS` option is an instruction to discard some redo information.

3.3 Oracle Database Backup Methodology

While Oracle provides users with a choice of several basic methods for making backups, we recommend that you use the Recovery Manager (RMAN) for Oracle Collaboration Suite. RMAN is a tool specifically designed to establish a connection with a server process and automate the movement of data for backup and recovery operations. It is a powerful and versatile program that allows users to make either an RMAN backup or an image copy of the data. RMAN automatically establishes the names and locations of all the files that need to be backed up, and can also use used for incremental backups, saving only those blocks of data that have changed since a previous backup.

The basic RMAN commands are `RESTORE` and `RECOVER`. RMAN can be used to restore datafiles from backup sets or image copes, either to their current location or to a new location. If any archived redo logs are required to complete the recovery operation, RMAN automatically restores and applies them. In a recovery catalog, RMAN keeps a record containing all the essential information concerning every backup ever taken. If a recovery catalog is not used, RMAN uses the control file for necessary information.

The RMAN `RECOVER` command can be used to perform complete media recovery and apply incremental backups, and to perform incomplete media recovery. If you specify files or archived logs using the RMAN `BACKUP` command, RMAN creates an output that is a backup set, or file(s) in a proprietary-specific format. This format requires the use of the RMAN `RESTORE` command for recovery operations. In contrast, when the `BACKUP AS COPY` command is used to create an image copy of a file, the copy is in an instance-usable format; you do not need to invoke RMAN to restore or recover it.

4 Understanding the Oracle Collaboration Suite Backup and Recovery Tool

To facilitate easy suite-level backup and recovery, Oracle recommends deploying the Oracle Collaboration Suite in the middle tier and using the **Oracle Collaboration Suite Backup and Recovery Tool**, a Perl script and associated configuration files that will automatically perform the following tasks:

- At a minimum, all users can refer to the tool for the list of configuration files that must be backed up.

- If you are new to backup and recovery, you can use the tool to automatically perform configuration file and infrastructure database backup and recovery.

- If you are experienced with backup and recovery, you can refer to the tool for guidance when setting up your own specific configuration file and infrastructure database backup and recovery scripts.

The Oracle Collaboration Suite Backup and Recovery Tool is not available in the standard Oracle Collaboration Suite installation.

You must download and configure the Oracle Collaboration Suite Backup and Recovery Tool for each installation in your Oracle Collaboration Suite environment, for the infrastructure installation and for the middle tier

installation. The reason you must download and configure the tool for all installations is that you will customize the tool for each one.

It is important to note that the Oracle Collaboration Suite Backup and Recovery Tool does not cover backing up and restoring of the following:

- Oracle Collaboration Suite software, such as binaries, oraInventory files, or Oracle system files (for example, /var/opt/oracle)

- User or application-specific user-defined files that are not part of the default installation, as described in Section 5, "Understanding Dynamic Plug-In Input Files"

- Any files owned by the root user

You will need to handle backup and recovery of these pieces separately, as required.

4.1 Downloading and Configuring the Oracle Collaboration Suite Backup and Recovery Tool

Step 1: Obtain the Oracle Collaboration Suite Backup and Recovery Tool

1. Point your browser to the Oracle Technology Network (OTN) Web site; the exact URL is:

   For **Unix**:

   http://download.oracle.com/otn/solaris/cs/10g/9iAS_BR.tar

   For **Windows**:

   http://download.oracle.com/otn/nt/cs/9042/9iAS_BR.zip

2. Download the *.zip file (for Windows) or *.tar file (for Unix platforms) for Oracle Collaboration Suite Backup and Recovery.

Step 2: Install the Oracle Collaboration Suite Backup and Recovery Tool

1. Create an empty directory in which to install the Oracle Collaboration Suite Backup and Recovery Tool. The directory can have any name you choose and can exist within the Oracle Collaboration Suite Oracle home or anywhere else on your system. The directory should be owned and writable by the operating system user who installed Oracle Collaboration Suite.

   To create a directory called BackupTool in the Oracle Collaboration Suite Oracle home, log in as the user who installed Oracle Collaboration Suite and perform:

   ```
   mkdir ORACLE_HOME/BackupTool
   ```

2. Once you un-zip or un-tar the downloaded file, move all files inside the backup_restore directory to the new ORACLE_HOME/BackupTool directory.

   - Make sure all files in the directory are owned by the user who installed Oracle Collaboration Suite.

   - For **Unix** only, make sure bkp_restore.pl has execute permission:

     ```
     chmod 755 bkp_restore.pl
     ```

3. Familiarize yourself with the Oracle Collaboration Suite Backup and Recovery Tool files. Instructions for editing the configuration files are in subsequent steps.

- **`bkp_restore.pl`**

  The Perl script that you execute to perform backup and recovery operations.

- **`config.inp`**

  The main configuration file that contains parameters for customizing the tool for your environment.

- **`config_component_files.inp`**

  Component configuration files. Each contains a list of configuration files for a particular component. These specify which files to back up when performing a configuration file backup.

- **`*.tmpl`**

  Templates for scripts for performing database backup and recovery operations using RMAN. When you initially configure the tool, a customized `*.dat` file will be created from each `*.tmpl` file.

- **`query_dbid.sql`**

  A SQL script called by the tool to initialize your configuration.

Step 3: Check Your Perl Installation

The Oracle Collaboration Suite Backup and Recovery Tool contains a Perl script, so you must have a Perl interpreter on your system and make sure it will work with the tool.

1. Make sure your system has a Perl installation of version 5.0 or above.

2. Make sure your Perl installation contains the Getopt module. If this module is not present, you will get an error of this type when you try to run the tool:

   ```
   Can't locate Getopt.pm in @INC
   ```

   If your Perl installation does not contain the Getopt module you can:

   - Download the module separately from the Comprehensive Perl Archive Network (CPAN):

     ```
     http://www.cpan.org
     ```

   - For **Windows** only, install the latest version of Active Perl:

     ```
     http://www.activestate.com/Products/ActivePerl
     ```

3. Make sure the tool can locate your Perl interpreter.

   On **Unix**,

   - Locate the Perl executable on your host:

     ```
     which perl
     ```

   - Edit the bkp_restore.pl file. In the first line, supply the full path to the Perl executable on your host:

     ```
     #!/usr/bin/perl -w
     ```

- You can then run the tool as follows:

```
cd BACKUP_TOOL_DIRECTORY
./bkp_restore.pl options
```

On **Windows**,

- Insert the Perl executable directory into your PATH environment variable. This directory is the same on infrastructure and middle tier installations:

```
ORACLE_HOME\perl\5.6.1\bin\MSwin32-x86
```

- You can then run the tool as follows:

```
cd BACKUP_TOOL_DIRECTORY
perl bkp_restore.pl options
```

Step 4: Create Backup Directories

Create directories to hold the various types of backup files:

- **Log files:** Log files for database backups and configuration file backups. Create this directory for middle tier and infrastructure installations.

- **Database backup files:** Datafile and control file backups of the database. Create this directory only if this is an infrastructure installation.

- **Configuration backup files:** These are file backups of the configuration files in the Oracle home. Create this directory for middle tier and infrastructure installations.

Oracle recommendations that you create backup directories as follows:

- Create your backup directories on a filesystem that is on a separate disk and, if possible, a separate disk controller, than your Oracle Collaboration Suite Oracle home. This will give you the best chance of recovering data in the event of a hardware failure.

- Allow enough disk space for your backups. Configuration file backups can use several hundred megabytes of space; database backups can use 1 or 2 gigabytes of space.

- Make sure your backup directories are writable by the user that installed Oracle Collaboration Suite.

For example, to create directories on /private for log files, database backup files, and configuration backup files:

On **Unix**,

```
mkdir -p /private/backups/log_files
mkdir -p /private/backups/db_files
mkdir -p /private/backups/config_files
cd /private/backups
chmod 755 log_files db_files config_files
chown Oracle9iAS_user log_files db_files config_files
```

On **Windows**,

```
mkdir C:\backups\log_files
mkdir C:\backups\db_files
mkdir C:\backups\config_files
```

Step 5: Perform Initial Configuration

Configure the Oracle Collaboration Suite Backup and Recovery Tool for your installation.

1. Edit `config.inp` and modify the parameters as described in the following list. Notice that some of the instructions are different depending on whether this is a middle-tier or infrastructure installation.

    ■   **oracle_home**

        Specify the full path of the Oracle home.

    ■   **log_path**

        The full path of the directory for log files.

    ■   **config_files_list**

        Do not insert a value for this; leave it as `config_files_list=DO_NOT_SET`.

        This parameter will be updated with the appropriate list of configuration files for your installation when you run `bkp_restore.pl -m configure`.

    ■   **config_backup_path**

        Specify the full path of the directory for configuration backup files.

    ■   **install_type**

        Do not insert a value for this; leave is as `install_type=DO_NOT_SET`.

        This parameter will be updated with the appropriate value for your installation when you run `bkp_restore.pl -m configure`.

    ■   **dbid**

        Do not insert a value for this; leave it as `dbid=DO_NOT_SET`.

        In infrastructure installations, this value will be updated with the infrastructure database `dbid` when you run `bkp_restore.pl -m configure`.

        In middle tier installations, this value will stay untouched.

    ■   **pfile**

        In middle tier installations, leave this line commented out.

        In infrastructure, if desired, specify an alternate `pfile` to use when starting up the database. Otherwise, leave the line commented out and the default pfile will be used:

        On **Unix**, *ORACLE_HOME*/dbs/initiasdb.ora

        On **Windows**, *ORACLE_HOME*/database/initiasdb.ora

        If you want to use the default, leave the `pfile` entry commented out; blank values are not allowed in this file.

    ■   **database_backup_path**

        In the middle tier installation, do not insert a value for this; leave it as `database_backup_path=VALUE_NOT_SET`.

In infrastructure, specify the full path of the directory for database backup files.

2. Set the ORACLE_HOME environment variable to the Oracle Collaboration Suite Oracle home.

3. If this is an infrastructure installation:

   - Set the ORACLE_SID environment variable to the infrastructure database SID. The default is iasdb.

   - Make sure the infrastructure database is started.

4. Update parameters in config.inp and, in the case of an infrastructure:

   On **Unix**,

   ```
   ./bkp_restore.pl -m configure
   ```

   On **Windows**,

   ```
   perl bkp_restore.pl -m configure
   ```

5. Oracle Collaboration Suite Backup and Recovery Tool will now create customized *.dat files that are used to perform backup, restore, and recovery on the database.

   > **Note:** You must run bkp_restore.pl -m config every time a change in the config.inp file is made in order for the changes to take effect.

4.2 Syntax of Oracle Collaboration Suite Backup and Recovery Tool

The syntax for the Oracle Collaboration Suite Backup and Recovery Tool is:

```
bkp_restore.pl [-defsv] -m mode [args]
```

The syntax supports the following options:

- **-d** Print a trace without executing.

- **-e** Specify an environment file; (default environment file is config.inp.)

- **-f** Force log file, database backup, and configuration file directories to be created if they do not exist.

- **-s** Run in silent mode.

- **-v** Run in verbose mode.

Use the **-m** option to specify which mode to run; some modes take arguments. The following listing describes the modes, their optional arguments, and their function.

- **configure [-e *env_file*]**

  Configures the tool.

  - If this is an infrastructure, make sure the database is running before you run this command.

- Reads the parameters specified in the default environment file (`config.inp`).With the `-e` option, uses the specified environment file instead.

- Updates `config_files_list` and `install_type` in `config.inp` with the appropriate files for your installation.

- If this is an infrastructure, queries the database id (`dbid`) and updates the configuration file and creates customized `*.dat` files from the database backup `*.tmpl` files.

- **backup_config [-e *env_file*]**

  Performs a configuration file backup.

  - Opens config.inp (unless the `-e` option was used) and retrieves `config_files_list`, `config_backup_path`, and `log_path`.

  - Attempts to open each file in `config_files_list` and `plugin_config_files_list`. Exits with an error if it cannot open all of the files.

  - For each file in `config_files_list` and `plugin_config_files_list`, checks if the first entry (the key file) exists. If the key file does not exist, assumes this component does not exist and moves on to the next component file. If the key file is found, backs up all files in the list. If a file other than a key file is not found, logs an error and continues.

  - When finished, stores the backup in `config_backup_path/config_bkp_*timestamp*`.

  - If any errors are encountered, creates a log file in `log_path/config_bkp_*timestamp*`.

- **restore_config [-e *env_file*] [-t config_bkp_*timestamp*]**

  Restores configuration files.

  - Opens config.inp (unless the `-e` option was used) and retrieves `config_backup_path` and `log_path`.

  - If the `-t` option is supplied, restores from that backup.

  - If the `-t` option is not supplied, displays a list of configuration backups in `config_backup_path` and exits.

  - Restores all files from the configuration backup to the Oracle home, preserving permissions and timestamp.

  - Performs `dcmctl updateConfig` to sync up DCM-related configuration files with the DCM repository.

  - If any errors are encountered, creates a log file in `log_path/config_rst_*timestamp*`.

- **backup_cold [-e *env_file*]**

  Performs a complete cold backup of the infrastructure database.

  - Opens `config.inp` (unless the `-e` option was used) and retrieves `log_path`.

  - Shuts down the database, starts it in mounted mode, but does not open it.

- Performs a backup of the datafiles and control files using RMAN. The commands are in `backup_cold.dat`.

- Stores the backup in the directory specified in `backup_cold.dat`. This is usually set to the `database_backup_path` in `config.inp`.

- Stores a log file in `log_path`.

- Opens the database.

- **`backup_cold_incr [-e env_file] -l incr_backup_level`**

  Performs an incremental cold backup of the infrastructure database.

  - Opens config.inp (unless the `-e` option was used) and retrieves `log_path`.

  - The `-l` option specifies the increment level (0-4).

  - Shuts down the database, starts it in mounted mode, but does not open it.

  - Performs a backup of the datafiles and control files using RMAN.

  - The commands are in `backup_cold_incrlevel.dat`.

  - Stores the backup in the directory specified in `backup_cold_incrlevel.dat`. This is usually set to the `database_backup_path` in `config.inp`.

  - Stores a log file in `log_path`.

  - Opens the database.

- **`backup_online [-e env_file]`**

  Performs an online backup of the infrastructure database.

  - Opens `config.inp` (unless the `-e` option was used) and retrieves `log_path`.

  - Assumes the database is open.

  - Performs a backup of the datafiles and control files using RMAN.

  - The commands are in `backup_online.dat`.

  - Stores the backup in the directory specified in backup_online.dat. (This is usually set to the `database_backup_path` in `config.inp`.)

  - Stores a log file in `log_path`.

  - Leaves the database open.

- **`backup_online_incr -l incr_backup_level`**

  Performs an incremental online backup of the infrastructure database.

  - Opens config.inp (unless the `-e` option was used) and retrieves `log_path`.

  - The `-l` option specifies the increment level (0-4).

  - Assumes the database is open.

  - Performs a backup of the datafiles and control files using RMAN.

  - The commands are in `backup_online_incrlevel.dat`.

- Stores the backup in the directory specified in
  `backup_online_incr`*`level`*`.dat`. (This is usually set to the
  `database_backup_path` in `config.inp`.)

- Stores a log file in `log_path`.

- Leaves the database open.

- **`restore_db [-e `*`env_file`*`] [-c]`**

  Restores and recovers the infrastructure database from the available cold and
  online backups.

  - Opens `config.inp` (unless the `-e` option was used) and retrieves
    `log_path`.

  - Assumes the database is shut down.

  - Restores the control files and datafiles, and performs recovery using
    RMAN. The commands are in `restore_db.dat`.

  - Stores a log file in `log_path`.

  - Leaves the database open.

  - The `-c` option restores the control file. By default, the control file is not
    restored. If you use the `-c` option, be sure to do a full backup right away,
    because all past backups are invalidated.

  - By default, this command searches for the most recent backup in the last
    7 days and recovers the database to the current time. You can modify this
    behavior as follows:

    – To begin the search on a day other than the current day, use the `SET`
      `UNTIL` command.

    – To search backwards for a number other than 7 days, use the
      `MAXDAYS` command. Refer to *Oracle9i Recovery Manager Reference* for
      details.

- **`help`**

  Prints a usage message.

5 Understanding Dynamic Plug-In Input Files

Oracle Collaboration Suite Backup and Recovery Tool places **dynamic plug-in
input files** into your *`ORACLE_HOME`*`/BackupTool` directory for all supported
Oracle Collaboration Suite components. Each dynamic plug-in input file specifies
the list of files that must be backed up for its Oracle Collaboration Suite
component.

You should note that your Oracle Collaboration Suite installation may not
contain **all** Oracle Collaboration Suite components. Additionally, the Oracle
Collaboration Suite Backup and Recovery Tool **does not automatically detect**
installed Oracle Collaboration Suite components. You must therefore enable the
Oracle Collaboration Suite Backup and Recovery Tool to access the files for the
installed Oracle Collaboration Suite components.

Because of expected interdependencies between data referenced in the dynamic
plug-in input file and other component configuration files in the same

ORACLE_HOME directory, all files must be combined into a single JAR archive for subsequent restore operations.

5.1 Formatting for Dynamic Plug-In Input Files

These naming conventions are used in the dynamic plug-in input files, `config_`*component_name*`_plugin.inp`, which is automatically installed by your Oracle Collaboration Suite Backup and Recovery Tool.

A dynamic plug-in input file would look like: `config_ocs_email_plugin.inp`.

The contents of a dynamic plug-in input file follow these formatting rules:

- To specify a single file, use this syntax:

  `$`*ORACLE_HOME*`/`*directory_path*`/`*file_name*

- To specify an entire directory, use this syntax:

  `$`*ORACLE_HOME*`/`*directory_path*`/`

- To specify files with a specific extension, use a wildcard `*` as in this syntax:

  `$`*ORACLE_HOME*`/`*directory_path*`/*.conf`

The first (or **key**) file listed in a dynamic plug-in input file must already exist, be accessible to the Oracle Collaboration Suite Backup and Recovery Tool, and cannot be listed using a wildcard. If the key file cannot be backed up, the backup configuration for that Oracle Collaboration Suite component will log an error message and continue to the next Oracle Collaboration Suite component:

`Key file `*key_file_name*` in `*plug_in_input_file_name*` does not exist`

5.2 Syntax for Using Dynamic Plug-In Input Files

A dynamic plug-in input file must be enabled before it can be used by the Oracle Collaboration Suite Backup and Recovery Tool. This enabling mode has the following syntax; you must specify the value of *component_name*, such as `ocs_email`.

On **Unix**,

```
./bkp_restore.sh [-dsv] -m enable_component_inp -y
   "component_name[[, ]component_name]"
```

On **Windows**,

```
bkp_restore.bat [-dsv] -m enable_component_inp -y
   "component_name[[, ]component_name]"
```

5.3 Notes on Using Dynamic Plug-In Input Files

- You must configure the Oracle Collaboration Suite Backup and Recovery Tool before enabling the use of dynamic plug-in input files. The names of all enabled dynamic plug-in input files are appended to the `plugin_config_files_list` in the main configuration file of the Oracle Collaboration Suite Backup and Recovery Tool, `config.inp`.

- To clear the entire `plugin_config_files_list` in the main configuration file, `config.inp`, you must re-configure the Oracle Collaboration Suite Backup and Recovery Tool.

- After enabling dynamic plug-in input files, you must perform a new backup configuration, `backup_config`, followed by a restore configuration, `restore_config`.

6 Understanding Calendar Backup and Recovery

The Calendar component provides command line utilities for backing up and restoring the database. These utilities can be used on their own, or they can be integrated into your existing environment and customized scripts used for backup and recovery. Note that in this release, the backup and recovery of the Calendar component is handled separately from other parts of the Oracle Collaboration Suite.

Oracle recommends that you follow a regular schedule of node and server maintenance because it provides the best protection against unscheduled down time and loss of data.

6.1 Calendar Maintenance Procedures

To minimize problems and ensure that the Calendar server runs smoothly and without interruption, you should perform these maintenance procedures.

6.1.1 Daily Monitoring and Maintenance Procedures

- Ensure that all relevant daemons and services are operational.

- Ensure that there is sufficient space in the `$ORACLE_HOME/ocal` directory or file system.

  > **See Also:**   Appendix A, "Disk Space and Memory in the *Oracle Calendar Administrator's Guide* for more information on calculating the storage requirements

- Verify that the previous night's backup completed successfully.

- Search for unusual entries in the log files in the `$ORACLE_HOME/ocal/log` directory, through primary logs `eng.log`, `lck.log`, `cws.log`, and `snc.log`. Make sure that you forward these results to the calendar server administrator. Alternatively, the run the unisnapshot utility to concatenate all the processes and error logs, including those for configuration files, into a single log `das.log`.

- Check for the presence of the `dbv.log` file in the directory `$ORACLE_HOME/ocal/log`. This file is created only if there are problems. If this file exists, analyze its contents and use the `unidbfix` utility to correct the problems. You should manually remove the `dbv.log` file once all problems are resolved.

  Your support provider can further assist you with problems identified in the `dbv.log` file.

- Perform a full backup of the calendar database, `$ORACLE_HOME/ocal/db`, and configuration files, `$ORACLE_HOME/ocal/misc`. This protects against

database corruption due to power failure or disk crashes in the event that your database cannot be restored.

Calendar maintenance can be performed through several interfaces:

6.1.1.1 Windows NT the **Performance Monitor** tool on Windows NT can be used to chart or log the performance and activity of Calendar services, wile the Event Viewer records all problems encountered during its operation.

6.1.1.2 Command Line To display the current status of the Calendar server, use the `unistatus` utility. To display the list of users that are logged onto the calendar server, use the `uniwho` utility. To determine just the number of users, include the `-nolist` option. To see all concurrent users who are connected to the Calendar server, use the `unilogons` utility (Unix only).

> **See Also:** Appendix E, "Utilities" in the *Oracle Calendar Reference Manual* for information on these utilities

6.1.1.3 Web GUI Calendar Administrator, an Internet-enabled tool, can show the Calendar server status. To see all servers on the network, click the **Server Administration** tab, followed by the **Servers** option. The **Actions** column indicates which servers are active and which ones are inactive. To examine a specific server, click the **View** icon in the **Actions** column. The **Identification** section displays the server status and the number of users currently logged on. This view also displays other server settings, such as whether user passwords can be changed, whether the server is connected to a Directory Server, and so on.

6.1.2 Weekly Monitoring and Maintenance Procedures

Oracle recommends that you perform the following system maintenances tasks on a weekly basis.

- Verify the consistency of the server databases running the `unidbfix` utility in check mode, while the Calendar server is running. All errors should be corrected immediately using `unidbfix` in fix mode; maintenance of most warnings can be delayed to the monthly maintenance schedule.

  Note that you don't need to shut down the entire system, but have the option to run `unidbfix` in fix mode on a single stopped node while the rest of the nodes are still active. Use the `-n` option to specify which nodes must be fixed. Additionally, multiple instances of the `unidbfix` utility can be run at the same time on different nodes.

- When using a directory server, run `unidsdiff` to detect and resolve any discrepancies that arise between the directory server and the calendar server when mapping users to resources in node. You may also synchronize your calendar and directory servers through the Calendar Administrator.

  You should also perform this task whenever you make a batch of changes to the calendar node, particularly when deleting users.

  > **See Also:** Appendix E, "Utilities" in the *Oracle Calendar Reference Manual* for information on the `unidibfix` and `unidsdiff` utilities

6.1.3 Monthly Monitoring and Maintenance Procedures

Oracle recommends that you perform the following system maintenance procedures on a monthly basis.

- Archive the log files. Remember to shut down the server before archiving the log files and to restart it once the task is completed.

- If you are using a directory server, synchronize it with the nodes by running `unidssync` as required.

- To improve performance and minimize disk space requirements, run the `unirmold` utility to remove all events and tasks older than 12-18 months.

- Ensure the consistence of the server databases by running the `unidbfix` utility in fix mode with the calendar server down. Correct all errors and warnings.

    > **See Also:** Appendix E, "Utilities" in the *Oracle Calendar Reference Manual* for information on the `unidssync`, `unirmold`, and `unidbfix` utilities

6.1.4 Additional Monitoring and Maintenance Options

The following options can be useful in automating Calendar server maintenance and improving its performance.

- The administrator can append text at the end of notification and reminder e-mail messages sent out by the Calendar server using the `[CWS]banner` parameter.

- You can collect statistical information on the Calendar server performance, relative user load at different times of the day and week, activity information of the `unicwsd` daemon, directory server access, and so on. This information is extremely useful for fine-tunning your maintenance, backup and recovery strategy of your enterprise. Turn on the following parameters for a short period of time, at regular intervals, and examine the resulting log files. Oracle recommends that these option be turned off once sufficient amount of statistical data is obtained.

    - To view elapsed time and CPU statistics for each client connection, set the parameter `[ENG] stats=TRUE` in the file `unison.ini`; when a client connection is closed, `stats` results are appended to the file `stats.log` in directory `$ORACLE_HOME/ocal/log`. Set the parameter `[ENG] stats` back to `FALSE` to disable logging when finished gathering data because this file grows very rapidly.

    - To gather statistics on log signons and signoffs to the Calendar server, set the parameter `[ENG] activity=TRUE`. The resulting `act.log` file in directory `$ORACLE_HOME/ocal/log` is useful for tracking server usage and for monitoring possible security violations. You should carefully monitor the size of the log file because it can grow quickly, and set the parameter back to `FALSE` to stop logging once finished.

    - To enable logging of failure errors, set the parameter `[ENG] dac_failederrlog=TRUE`. The contents of the file `eng.log` in directory `$ORACLE_HOME/ocal/log` will then indicate the presence of errors related to directory server access that appear in the client interface as "unexpected error".

- To determine whether activity information of the `unicwsd` daemon are logged for the modules specified in the list `log_modulesinclude`, set the `[CWS] log_activity=TRUE`. The results are stored in file `cws.log` in directory `$ORACLE_HOME/ocal/log`. Make sure to set the parameter `[CWS] log activity` back to `FALSE` to disable logging when finished gathering data because this file grows very rapidly.

  See Also: Appendix C, "Calendar Server Parameters" of the *Oracle Calendar Reference Manual* for information on these parameters.

6.2 Calendar Backup

To copy the Calendar database to a specified location, use the online backup utility **unidbbackup**. This operation creates a backup of a single Calendar server node and its related configuration information. More specifically, it backs up the *ORACLE_HOME*/`ocal/misc` and *ORACLE_HOME*/`ocal/db` directories. Because the data in these two directories is interdependent, it is important to ensure they are backed up at the same time. As its last step, `unidbbackup` rotates the saved database to a tape backup.

By default, the `unidbbackup` utility performs a copy of the source to the destination. If you require something other than a straight copy, alternative external backup choices can be invoked through the `unidbbackup` utility.

You should note that `unidbbackup` backs up the Calendar server internal database. If you are using a directory server, its database should also be backed up at the same time.

Note that the `unidbbackup` utility can be used when the Calendar server is either up or down.

6.3 Calendar Recovery

The Calendar server can be restored by using a complement to `unidbbackup`, the **unidbrestore** utility. This operation restores a single node and related configuration information of a Calendar server from a backup made earlier by `unidbbackup`. By default, the destination directory for the restore is *ORACLE_HOME*/`ocal`, which means that the restore utility overwrites the existing files of the Calendar server database. Therefore, you should use unidbrestore with extreme care and ensure that the Calendar server database is not inadvertently corrupted. You may chose to use the `-d` option to specify a different directory for the restore, and then copy the individual files from the restored directory into the *ORACLE_HOME*/`ocal` directory.

Because unidbrestore restores the Calendar server's internal database, if the directory server is used in your deployment, its database is not backed up. Therefore, if a Calendar server node is restored after some users have been deleted, these users must be added back into the directory server. Similarly, if a single node is restored after its network information is changed, the database may encounter conflicts between the current network configuration and the restored node's old network information, which results in errors.

Note that unlike `unidbbackup`, the `unidbrestore` utility can only be used when the Calendar server is down.

6.4 Restoring a Single Calendar User

If you need to restore a single user account, run the **unirestore** utility to extract this information from a backup previously made by the unidbbackup utility.

> **See Also:** The following documents for a detailed information on how to implement a backup and recovery strategy for the Calendar component of your Oracle Collaboration Suite deployment:
>
> - Chapter 15, "Node Maintenance" in *Oracle Calendar Administrator's Guide*, In particular, read the sections on "Server backup and restore" and "User backup and restore".
>
> - Appendix F, "Calendar server utilities" in *Oracle Calendar Reference Manual*. In particular, read the sections on:
>
>   - unidbbackup: online backup utility
>
>   - unidbrestore: recovery of an entire Calendar database
>
>   - unirestore: recovery of a single calendar user
>
>   - uniarch: TAR archive utility (for **Unix** only)
>
>   - unirmold: removes Calendar data based on date and tasks
>
>   - unisnapshot: compiles calendar server information for diagnostics

7 Oracle Collaboration Suite Backup and Recovery Procedures

This section describes the various procedures involved in backup and recovery of the Oracle Collaboration Suite, including the middle tier, the infrastructure and the infostore. In general, you should use either customized scripts or RMAN to perform backup and recovery operations on the infostore tier.

You should note that in this release the backup and recovery of the Calendar component is handled separately, as described in Section 6, "Understanding Calendar Backup and Recovery".

This section contains the following topics:

- Backup and Recovery Procedures

- Using the Oracle Collaboration Suite Backup and Recovery Tool for Configuration Files

- Database Backup and Restore

- Oracle Collaboration Suite Backup Procedures

- Restore and Recovery for Data Loss, Host Failure, or Media Failure

- Recovery Strategies for Process or System Outages and Crashes

- Starting and Stopping the Oracle Collaboration Suite Environment

7.1 Backup and Recovery Procedures

The following list summarizes the backup and recovery procedures mentioned in the previous section and show which ones you can perform with the tool.

- **Backing up the middle tier Oracle home** Use standard OS utilities like `tar`, `copy` or `cpio`.

- **Backing up the infrastructure Oracle home** Use standard OS utilities like `tar`, `copy` or `cpio`.

- **Backing up the infostore Oracle home** Use standard OS utilities like `tar`, `copy` or `cpio`.

- **Performing a complete cold backup of the infrastructure** You can use the Oracle Collaboration Suite Backup and Recovery Tool for this, or refer to the tool and develop your own scripts.

- **Performing a complete cold backup of the infostore** Use RMAN or customized scripts to backup the database.

- **Backing up Oracle system files** Use standard OS utilities like `tar`, `copy` or `cpio`.

- **Backing up the configuration files in the middle tier Oracle home** You can use the Oracle Collaboration Suite Backup and Recovery Tool for this, or refer to the tool and develop your own scripts.

- **Backing up the configuration files in the infrastructure Oracle home** You can use the Oracle Collaboration Suite Backup and Recovery Tool for this, or refer to the tool and develop your own scripts.

- **Backing up the configuration files in the infostore Oracle Home** Use standard OS utilities like `tar`, `copy` or `cpio`.

- **Performing an online backup of the infrastructure** You can use the Oracle Collaboration Suite Backup and Recovery Tool for this, or refer to the tool and develop your own scripts.

- **Performing an online backup of the infostore** Use RMAN or customized scripts to backup the database.

- **Restoring Oracle static binaries or libraries from a complete cold backup** Use standard OS utilities like `tar`, `copy` or `cpio`.

- **Restoring configuration files from your most recent partial online backup** You can use the Oracle Collaboration Suite Backup and Recovery Tool for this, or refer to the tool and develop your own scripts.

- **Restoring and recovering the infrastructure to its latest state** You can use the Oracle Collaboration Suite Backup and Recovery Tool for this, or refer to the tool and develop your own scripts.

- **Restoring and recovering the infostore to its latest state** Use RMAN or customized scripts to backup the database.

7.2 Using the Oracle Collaboration Suite Backup and Recovery Tool for Configuration Files

A configuration file backup is a filesystem backup of all configuration files in a middle tier or infrastructure Oracle home.

7.2.1 Customizing the Oracle Collaboration Suite Backup and Recovery Tool for Configuration Files

Before you customize the tool, you should understand how it works. When you use the tool to back up your configuration files, it:

1. Opens `config.inp` (unless another environment file was specified with the `-e` option) and retrieves the `config_files_list` (static files) and the `plugin_config_files_list` (dynamic plug-in input files). These files contain the names of the configuration files that apply to your installation.

   The static files have the following name format:

   `config_component_files.inp`

   The dynamic files have the following name format:

   `config_ocs_component_plugin.inp`

2. Attempts to open each file in `config_files_list` and the `plugin_config_files_list`. Exits with an error if it cannot open all of the files.

3. The first entry in each configuration file of a dynamic list is the **key file**, used to determine if the component is in this installation. If the tool finds the key file, it knows the component is installed, and attempts to back up all of the entries in the configuration file. It logs an error whenever it cannot find a specific file.

   If the key file does not exist, the tool does not attempt to back up any files for that component. It logs an error and skips to the plugin input file of the next Oracle Collaboration Suite component.

You must customize the tool is to add your own local configuration files:

1. Add entries to the `config_misc_files.inp` file.

2. Make sure that the first entry in the file (the key file) is a file that will always exist in your installation.

3. Add as many entries to the file as you like.

The `config_misc_files.inp` file is always included in the `config_files_list` in parameter in `config.inp`, so there is no need to edit `config.inp`.

7.2.2 Backing Up Configuration Files

To back up the configuration files in a middle-tier or infrastructure installation:

1. Change directory to the Oracle Collaboration Suite Backup and Recovery Tool directory for the Oracle home you would like to back up. For example:

   `cd ORACLE_HOME/BackupTool`

2. Start the database and the listener, and then perform the following commands:

   ```
   oidmon start
   oidctl server=oidldapd instance=1 start
   $ORACLE_HOME/opmn/bin/opmnctl start
   $ORACLE_HOME/opmn/bin/opmnctl startproc type=ohs
   $ORACLE_HOME/opmn/bin/opmnctl startproc type=oc4j gid=OC4J_DAS
   $ORACLE_HOME/dcm/bin/dcmctl updateconfig -d -v
   ```

3. Run the following command. Use the `-v` option to see the list of files that are backed up. You may want to first run the command with the `-d` option to preview the results and determine if there will be any errors.

On **Unix**,.

```
/bkp_restore.pl [-v] -m backup_config
```

On **Windows**,

```
perl bkp_restore.pl [-v] -m backup_config
```

When finished, the command prints the name of the directory in which it stored the backup. This directory has a timestamp in its name. If any errors occurred, it prints the name of the log file that contains the error messages. The log file has the same timestamp.

7.2.3 Restoring Configuration Files

You should implement the following tasks both for the infrastructure and for the middle tier:

1. Change directory to the Oracle Collaboration Suite Backup and Recovery Tool directory for the Oracle home you would like to back up. For example:

```
cd ORACLE_HOME/BackupTool
```

2. Run the following command. Use the `-v` option to see the list of files that are restored:

On **Unix**,

```
./bkp_restore.pl [-v] -m restore_config -t backup_dir_name
```

On **Windows**,

```
perl bkp_restore.pl [-v] -m restore_config -t backup_dir_name
```

The tool copies all files in the backup to the Oracle home. If any errors occurred, it prints the name of the log file that contains the error messages. After all files have been restored, the tool performs dcmctl updateConfig to sync up the DCM-related configuration files with the DCM repository.

7.3 Database Backup and Restore

This section deals with particulars of cold database backup, online database backup, and restoring a database using the Oracle Collaboration Suite Backup and Recovery Tool.

7.3.1 Performing Cold Database Backups

1. Leave the database open. The tool will take care of stopping it and starting it again when finished.

2. Set the `ORACLE_HOME` environment variable to the infrastructure Oracle home.

3. Set the `ORACLE_SID` environment variable to the infrastructure SID. The default is `iasdb`.

4. Change directory to the Oracle Collaboration Suite Backup and Recovery Tool directory for the infrastructure Oracle home:

   ```
   cd ORACLE_HOME/BackupTool
   ```

5. Run the following command. Use the -v option to see the list of files that are backed up. This command stores a datafile backup and a control file backup in the database_backup_path specified in config.inp. It also stores timestamped log files in log_path.

   On **Unix**,

   ```
    ./bkp_restore.pl -m backup_cold
   ```

   On **Windows**,

   ```
   perl bkp_restore.pl -m backup_cold
   ```

6. To backup the infostore database, use RMAN or customized scripts.

7.3.2 Performing Online Database Backups

1. Leave the database open.

2. Set the ORACLE_HOME environment variable to the infrastructure Oracle home.

3. Set the ORACLE_SID environment variable to the infrastructure SID. The default is iasdb.

4. Change directory to the Oracle Collaboration Suite Backup and Recovery Tool directory for the infrastructure Oracle home.

   ```
   cd ORACLE_HOME/BackupTool
   ```

5. Run the following command. Use the -v option to see the list of files that are backed up. This command stores a datafile backup and a control file backup in the database_backup_path specified in config.inp. It also stores timestamped log files in log_path.

   On **Unix**,

   ```
    ./bkp_restore.pl -m backup_online
   ```

   On **Windows**,

   ```
   perl bkp_restore.pl -m backup_online
   ```

6. To backup the infostore database, use RMAN or customized scripts.

7.3.3 Restoring a Database

1. Shut down the database.

2. Set the ORACLE_HOME environment variable to the infrastructure Oracle home.

3. Set the ORACLE_SID environment variable to the infrastructure SID. The default is iasdb.

4. Change directory to the Oracle Collaboration Suite Backup and Recovery Tool directory for the infrastructure Oracle home.

   ```
   cd ORACLE_HOME/BackupTool
   ```

5. Restore the database:

   On **Unix**,

   ```
   ./bkp_restore.pl -m restore_db
   ```

   On **Windows**,

   ```
   perl bkp_restore.pl -m restore_db
   ```

6. To restore the infostore database, use RMAN or customized scripts.

7.4 Oracle Collaboration Suite Backup Procedures

The basic outline of backup procedures follows.

1. Immediately after you install Oracle Collaboration Suite,

   - Download and configure the Oracle Collaboration Suite Backup and Recovery Tool, as described in Section 4.1, "Downloading and Configuring the Oracle Collaboration Suite Backup and Recovery Tool".

   - Set up RMAN or customized scripts for backup and recovery of the infostore; see Section 3.3, "Oracle Database Backup Methodology".

   - Enable ARCHIVELOG mode in the infrastructure and infostore databases, as described in Section 7.4.1, "Enabling ARCHIVELOG Mode".

   - Create a record of your Oracle Collaboration Suite environment, as described in Section 7.4.2, "Creating a Record of Your Oracle Collaboration Suite Configuration".

   - Perform a complete cold backup of your Oracle Collaboration Suite environment, as described in Section 7.4.3, "Performing a Complete Cold Backup of Your Oracle Collaboration Suite Environment".

   - Perform regular partial online backups of your Oracle Collaboration Suite environment, as described in Section 7.4.4, "Performing a Partial Online Backup of Your Oracle Collaboration Suite Environment".

2. Whenever you need to upgrade or patch Oracle Collaboration Suite or your operating system,

   - Update the record of your Oracle Collaboration Suite environment, as described in Section 7.4.2, "Creating a Record of Your Oracle Collaboration Suite Configuration".

   - Perform a complete cold backup of your Oracle Collaboration Suite environment, as described in Section 7.4.3, "Performing a Complete Cold Backup of Your Oracle Collaboration Suite Environment".

   - Perform regular online backups of your Oracle Collaboration Suite environment, as described in Section 7.4.4, "Performing a Partial Online Backup of Your Oracle Collaboration Suite Environment".

3. Additional tips:

   - Create a backup of the JRE/JDK on your system. This isn't an Oracle product, but it is utilized by Oracle Collaboration Suite and, if accidentally lost or corrupted, would need to be restored in order for Oracle Collaboration Suite to function. This issue applies to HP-UX, HP Tru64, and IBM AIX systems.

- Make sure your backups are valid by routinely verifying that they can be restored.

7.4.1 Enabling ARCHIVELOG Mode

By default, the infrastructure and infostore do not have ARCHIVELOG mode enabled. You should enable ARCHIVELOG mode before you perform your first complete cold backup. Otherwise, your backup control files will contain the NOARCHIVELOG mode setting. These steps should be used for both the infrastructure and the infostore.

To enable ARCHIVELOG mode:

Step 1: Set up archive logging parameters

On **Unix**, edit the file *INFRA_ORACLE_HOME*/dbs/init.ora:

1. Uncomment the following line by removing the initial '#' character so it appears like this:

    ```
    log_archive_start = true
    ```

2. [Optional] The default destination directory for archive logs is *INFRA_ORACLE_HOME*/rdbms. If you would like to use a different directory, uncomment the following line and specify the directory:

    ```
    log_archive_dest = '/disk1/archive'
    ```

3. [Optional] The default filename format for archive logs is TthreadSsequence.ARC. If you would like to use a different format, uncomment the following line and specify a format:

    ```
    log_archive_format = arch%s.arc
    ```

    On **Windows**, edit the file:

    ```
    INFRA_ORACLE_HOME\..\admin\iasdb\pfile\init.ora
    ```

4. Add the following line anywhere in the file:

    ```
    log_archive_start = true
    ```

5. [Optional] The default destination directory for archive logs is *INFRA_ORACLE_HOME*\rdbms. If you would like to use a different directory, add the following line and specify the directory:

    ```
    log_archive_dest = ' C:\database_archives\'
    ```

6. [Optional] The default filename format for archive logs is TthreadSsequence.ARC. If you would like to use a different format, add the following line and specify a format:

    ```
    log_archive_format = arch%s.arc
    ```

Step 2: Set the ORACLE_HOME and Oracle_SID variables

Make sure the ORACLE_HOME and ORACLE_SID environment variables are properly set; the default is iasdb.

Step 3: Check for active users

Make sure nobody is using the database.

Step 4: Shut down database

Perform a clean, normal shutdown of the database instance.

```
INFRA_ORACLE_HOME/bin/sqlplus /nolog
SQL> connect sys/password as sysdba
SQL> shutdown
```

Step 5: Start up the database

Start up the instance and mount, but do not open, the database.

```
SQL> startup mount;
```

Step 6: Turn on ARCHIVELOG

Enable database ARCHIVELOG mode.

```
SQL> alter database archivelog;
SQL> alter system set log_archive_start=true scope=spfile;
```

Step 7: Shut down and restart database

Shut down and restart the database instance.

```
SQL> shutdown
SQL> startup
```

Step 8: Verify that ARCHIVELOG is on

Verify the database is now in ARCHIVELOG mode. Execute the following command and verify that the database log mode is 'Archive Mode' and automatic archival is enabled.

```
SQL> archive log list;
Database log mode Archive Mode
Automatic archival Enabled
Archive destination /private/oraocs/dbs/arch
Oldest on-line log sequence 19
Next log sequence to archive 21
Current log sequence 21
```

> **See Also:** *Oracle9i Database Administrator's Guide Release 1 (9.0.1)* for more detailed information on the parameters in this section, and on setting up archive logging in general.

7.4.2 Creating a Record of Your Oracle Collaboration Suite Configuration

In the event you need to restore and recover your Oracle Collaboration Suite environment, it is important to have all the necessary information at your disposal. This is especially true in the event of a hardware loss that requires you to reconstruct all or part of your Oracle Collaboration Suite environment on a new disk or host.

You should maintain an up-to-date record of your Oracle Collaboration Suite environment that includes the information listed in this section. You should keep this information both in hardcopy and electronic form. The electronic form

should be stored on a host or email system that is completely separate from your Oracle Collaboration Suite environment.

Your Oracle Collaboration Suite hardware and software configuration record should include the following information:

Host   For each host in your environment, include:

- Hostname
- Virtual hostname, if any
- Domain name
- IP address
- Hardware platform
- Operating system release level and patch information

Oracle Collaboration Suite   For each Oracle Collaboration Suite installation in your environment, include:

- Installation type (Infrastructure, J2EE and Web Cache, Portal and Wireless)
- Host on which the installation resides
- Amount of disk space used by the installation
- Port numbers used by the installation
- On a **Unix** system,
    - User name, userid number, group name, groupid number, environment profile, and type of shell for the operating system user that owns the Oracle home (`/etc/passwd` and `/etc/group` entries)
    - Directory structure, mount points, and full path for `ORACLE_HOME`

Infrastructure and Infostore   For infrastructure and infostore databases, include:

- Database version and patch level
- Base language
- Character set
- Database name
- SID

7.4.3 Performing a Complete Cold Backup of Your Oracle Collaboration Suite Environment

This section describes how to perform an complete cold backup of your Oracle Collaboration Suite environment. The steps are:

Step 1: Shut down your Oracle Collaboration Suite Environment

1. Stop the middle tier instance by following steps in Section 7.7.2, "Stopping the Middle Tier Instance"

2. Stop the infrastructure by following steps in Section 7.7.4, "Stopping the Infrastructure".

3. Stop the infostore by following steps in Section 7.7.6, "Stopping the Infostore"

Step 2: Back up the infrastructure

1. Perform a cold database backup of the infrastructure database using either your own procedures or the Oracle Collaboration Suite Backup and Recovery Tool. Before performing the cold database backup, leave the database open. The tool will take care of stopping it and starting it again when finished:

   ```
   cd INFRA_BACKUP_TOOL_DIRECTORY
   ```

   On **Unix**,

   ```
   ./bkp_restore.pl -m backup_cold
   ```

   On **Windows**,

   ```
   perl bkp_restore.pl -m backup_cold
   ```

2. Perform a complete backup of all files in the infrastructure Oracle home using your preferred operating system command, such as `tar` or `cpio`.

   Be sure to perform this backup as root because some of the files in the Oracle home are owned by root. It is important to perform the backup so that file owners, groups, permissions, and timestamps are preserved.

   ```
   cd INFRA_ORACLE_HOME
   tar cvf full_path_of_backup_file .
   ```

3. Perform a backup of all configuration files in the infrastructure Oracle home. The reason for doing a configuration file backup immediately after backing up the entire Oracle home is that it provides a snapshot of your initial configuration files, in case you start to reconfigure your system and then would like to restore the configuration files to their original state.

   For example, to do this using the Oracle Collaboration Suite Backup and Recovery Tool:

   ```
   cd INFRA_BACKUP_TOOL_DIRECTORY
   ```

   On **Unix**,

   ```
   ./bkp_restore.pl -m backup_config
   ```

   On **Windows**,

   ```
   perl bkp_restore.pl -m backup_config
   ```

Step 3: Back up the infostore

To backup the infostore database, use RMAN or customized scripts.

Step 4: Back up the middle tier

1. Perform a complete backup of all files in the middle-tier Oracle home using your preferred operating system command, such as tar or cpio. Be sure to perform this backup as root because some of the files in the Oracle home are owned by root. It is important to perform the backup so that file owners, groups, permissions, and timestamps are preserved. For example:

   ```
   cd MID_TIER_ORACLE_HOME
   tar cvf full_path_of_backup_file .
   ```

2. Perform a backup of all configuration files in the middle tier Oracle home. The reason for doing a configuration file backup immediately after backing up the entire Oracle home is that it provides a snapshot of your initial configuration files, in case you start to reconfigure your system and then would like to restore the configuration files to their original state.

To do this using the Oracle Collaboration Suite Backup and Recovery Tool:

```
cd MID_TIER_BACKUP_TOOL_DIRECTORY
```

On **Unix**,

```
./bkp_restore.pl -m backup_config
```

On **Windows**,

```
perl bkp_restore.pl -m backup_config
```

Step 4: Back up your Oracle system files

On each host in your Oracle Collaboration Suite environment:

1. Make a backup of your Oracle system files using your preferred operating system command, such as `tar` or `cpio`. Consult your OS-specific documentation to determine which directory contains the Oracle system files.

On **Unix**, they may be in the `/etc` or the `/var/opt/oracle` directory.

2. If the `oraInventory` directory resides outside of your Oracle Collaboration Suite Oracle home, make a backup of it using your preferred operation system command, such as tar or cpio. Consult your OS-specific documentation to determine the location of the oraInventory directory.

On **Unix**, the location of the `oraInventory` directory may be listed in `/etc/oraInst.loc` or `/var/opt/oracle/oraInst.loc`.

On **Windows**, the location of the oraInventory directory can be obtained from the registry `HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE\INST_LOC`.

Step 5: Start your Oracle Collaboration Suite environment

1. Start the infrastructure, as described in Section 7.7.3, "Starting the Infrastructure".

2. Start the infostore, as described in Section 7.7.5, "Starting the Infostore"

3. Start the middle tier instance, as described in Section 7.7.1, "Starting the Middle Tier Instance".

7.4.4 Performing a Partial Online Backup of Your Oracle Collaboration Suite Environment

Perform subsequent partial online backups at regular intervals.These backups only contain configuration files, the infrastructure and the infostore.

You can set up a regularly scheduled job that performs a partial online backup. The frequency with which you perform a backup depends on how often you perform administrative operations on your Oracle Collaboration Suite environment, such as changing passwords, changing configuration parameters, installing new components, or deploying new applications.

Step 1: Back up the infrastructure

You can leave all infrastructure processes running while you perform this step.

1. Perform a backup of all configuration files in the infrastructure Oracle home. To do this using the Oracle Collaboration Suite Backup and Recovery Tool:

    ```
    cd INFRA_BACKUP_TOOL_DIRECTORY
    ```

    On **Unix**,

    ```
    ./bkp_restore.pl -m backup_config
    ```

    On **Windows**,

    ```
    perl bkp_restore.pl -m backup_config
    ```

2. Perform an online database backup of the infrastructure database. You can perform this step using your own procedures or the Oracle Collaboration Suite Backup and Recovery Tool:

    ```
    cd INFRA_BACKUP_TOOL_DIRECTORY
    ```

    On **Unix**,

    ```
    ./bkp_restore.pl -m backup_online
    ```

    On **Windows**,

    ```
    perl bkp_restore.pl -m backup_online
    ```

Step 2: Back up the Infostore

To backup the infostore database, use RMAN or customized scripts.

Step 3: Back up the Middle Tier

You can leave all middle tier processes running while you perform this step. Perform a backup of all configuration files in the middle tier Oracle home. To do this using the Oracle Collaboration Suite Backup and Recovery Tool:

```
cd MID_TIER_BACKUP_TOOL_DIRECTORY
```

On **Unix**,

```
./bkp_restore.pl -m backup_config
```

On **Windows**,

```
perl bkp_restore.pl -m backup_config
```

7.5 Restore and Recovery for Data Loss, Host Failure, or Media Failure

This section describes restore and recovery methods for outages that involve actual data loss or corruption, host failure, or media failure where the host or disk cannot be restarted and are permanently lost. This type of failure requires some type of data restoration before the Oracle Collaboration Suite environment can be restarted and continue with normal processing.

The following procedures assume that:

- ARCHIVELOG mode was enabled for all infrastructure and infostore backups.

- No administrative changes were made since the last backup. If administrative changes were made since the last backup, they will need to be reapplied after restore and recovery is complete. Administrative changes include any operations that result in changes to configuration files or the infrastructure database, such as changing configuration parameters, passwords, or applications.

- Complete recovery of the database can be performed; no redo log files have been lost.

When the loss happens in the **infrastructure** tier,

- If any Oracle binaries have been lost or corrupted, you must recover the entire infrastructure, as described in Section 7.5.1, "Restoring an Infrastructure to the Same Host".

- If the infrastructure database is corrupted due to data loss or media failure, you can restore and recover it, as described in Section 7.5.2, "Restoring and Recovering the Infrastructure".

- If you lose any configuration files in the infrastructure Oracle home, you can restore them, as described in Section 7.5.4, "Restoring Infrastructure Configuration Files".

- If you lose some configuration files and the infrastructure database is corrupted, you can restore and recover both, as described in Section 7.5.4, "Restoring Infrastructure Configuration Files" and Section 7.5.2, "Restoring and Recovering the Infrastructure".

When the loss happens in the **infostore** tier, use RMAN or customized scripts.

When the loss happens in the **middle tier**,

- If any Oracle binaries have been lost or corrupted, you must restore the entire middle tier to the same host, as described in Section 7.5.5, "Restoring a Middle Tier to the Same Host"

- If you lose any configuration files in the middle tier Oracle home, you can restore them., as described in Section 7.5.6, "Restoring Middle Tier Configuration Files".

7.5.1 Restoring an Infrastructure to the Same Host

This section describes how to restore and recover an infrastructure to the same host. Use this procedure when you have lost some or all of your Oracle binaries.

Step 1: Stop the infrastructure

Follow the steps in Section 7.7.4, "Stopping the Infrastructure"

Step 2: Stop the infostore

Follow the steps in Section 7.7.6, "Stopping the Infostore"

Step 3: Restore the infrastructure Oracle home

1. Restore the backup (tar, cpio) of the infrastructure Oracle home from your complete cold backup. Be sure your method of restoring the files preserves the original owner, group, permissions, and timestamps. To do this using the Oracle Collaboration Suite Backup and Recovery Tool:

   ```
   cd BACKUP_TOOL_DIRECTORY
   ```

On **Unix**,

```
./bkp_restore.pl -m restore_config -t config_bkp_timestamp
```

On **Windows**,

```
perl bkp_restore.pl -m restore_config -t config_bkp_timestamp
```

2. Restore the configuration file backup from your most recent partial online backup.

Step 4: Restore the infostore Oracle home

Use RMAN or customized scripts.

Step 5: Restore and recover the infrastructure

Restore and recover the infrastructure database from your latest backup. To do this using the Oracle Collaboration Suite Backup and Recovery Tool:

```
cd BACKUP_TOOL_DIRECTORY
```

On **Unix**,

```
./bkp_restore.pl -m restore_db
```

On **Windows**,

```
perl bkp_restore.pl -m restore_db
```

Step 6: Restore and recover the infostore

Use RMAN or customized scripts.

Step 7: Start the infrastructure

Follow the steps in Section 7.7.3, "Starting the Infrastructure".

Step 8: Start the infostore

Follow the steps in Section 7.7.5, "Starting the Infostore".

7.5.2 Restoring and Recovering the Infrastructure

If only the infrastructure has been corrupted, and other files in the Oracle home are not damaged, you should restore and recover the infrastructure database from your latest backup using your own procedures, or the Oracle Collaboration Suite Backup and Recovery Tool:

```
cd BACKUP_TOOL_DIRECTORY
```

On **Unix**,

```
./bkp_restore.pl -m restore_db
```

On **Windows**,

```
perl bkp_restore.pl -m restore_db
```

7.5.3 Restoring and Recovering the Infostore

Use RMAN or customized scripts.

7.5.4 Restoring Infrastructure Configuration Files

This section describes how to restore the configuration files in an infrastructure Oracle home. Use this procedure when any configuration files have been lost or corrupted.

Step 1: Stop the infrastructure

Follow the steps in Section 7.7.4, "Stopping the Infrastructure".

Step 2: Restore configuration files

Restore the configuration files from your most recent partial online backup. To do this using the Oracle Collaboration Suite Backup and Recovery Tool:

```
cd BACKUP_TOOL_DIRECTORY
```

On **Unix**,

```
./bkp_restore.pl -m restore_config -t config_bkp_timestamp
```

On **Windows**,

```
perl bkp_restore.pl -m restore_config -t config_bkp_timestamp
```

Step 3: Apply recent administrative changes

If you made any administrative changes since the last time you did a partial online backup, reapply them now.

Step 4: Start the infrastructure

Follow the steps in Section 7.7.3, "Starting the Infrastructure"

7.5.5 Restoring a Middle Tier to the Same Host

This section describes how to restore a middle tier to the same host. Use this procedure when you have lost some or all of your Oracle binaries.

Step 1: Stop the middle tier instance

Follow the steps in Section 7.7.2, "Stopping the Middle Tier Instance".

Step 2: Make sure the infrastructure is up

If the middle tier is associated with an infrastructure, make sure the infrastructure is up and running while you restore the middle tier. This is because there is a step in the recovery procedure that involves syncing up configuration files between the middle tier and the infrastructure.

Step 3: Restore the middle tier Oracle home

1. Restore the backup (tar, cpio) of the middle tier Oracle home from your complete cold backup. Be sure your method of restoring the files preserves the original owner, group, permissions, and timestamps.

2. Restore the configuration file backup from your most recent partial online backup. To do this using the Oracle Collaboration Suite Backup and Recovery Tool:

    ```
    cd BACKUP_TOOL_DIRECTORY
    ```

    On **Unix**,

```
./bkp_restore.pl -m restore_config -t config_bkp_timestamp
```

On **Windows**,

```
perl bkp_restore.pl -m restore_config -t config_bkp_timestamp
```

Step 4: Start the middle tier

Follow the steps in Section 7.7.1, "Starting the Middle Tier Instance".

7.5.6 Restoring Middle Tier Configuration Files

This section describes how to restore the configuration files in a middle-tier Oracle home. Use this procedure when any configuration files have been lost or corrupted.

Step 1: Stop the middle tier

Follow the steps in Section 7.7.2, "Stopping the Middle Tier Instance".

Step 2: Restore configuration files

Restore the configuration files from your most recent partial online backup. To do this using the Oracle Collaboration Suite Backup and Recovery Tool:

```
cd BACKUP_TOOL_DIRECTORY
```

On **Unix**,

```
./bkp_restore.pl -m restore_config -t config_bkp_timestamp
```

On **Windows**,

```
perl bkp_restore.pl -m restore_config -t config_bkp_timestamp
```

Step 3: Apply recent administrative changes

If you made any administrative changes since the last time you did a partial online backup, reapply them now.

Step 4: Start the middle tier

Follow the steps in Section 7.7.1, "Starting the Middle Tier Instance".

7.6 Recovery Strategies for Process or System Outages and Crashes

This section describes recovery strategies for process or system outages and crashes. These types of outages do not involve any data loss, and therefore do not require any files to be restored or recovered. In some cases, failure may be transparent and no manual intervention is required to restore the failed component. However, in some cases, manual intervention is required to restart a process or component.

While these strategies do not strictly fit into the category of backup and recovery, they are included in this document for completeness.

When determining which restore and recovery strategy to use, you should identify the scope of loss (middle tier or infrastructure), identify the type of loss, and follow the recovery strategy. The strategies refer to specific recovery procedures. If the loss occurred in both the infrastructure and middle tier, follow the infrastructure recovery strategy first, then the middle tier recovery strategy.

7.6.1 Infrastructure Tier, Host Lost, No Data Loss

To restart:
1. Reboot the host.
2. Follow the steps in Section 7.7.3, "Starting the Infrastructure".

7.6.2 Infrastructure Tier, Database Instance Failure (Crash)

To check status:
1. Try connecting to the database using SQL*Plus.
2. Check the state as follows:

```
SQL> select status from v$instance;
```

To restart:
```
ORACLE_HOME/bin/sqlplus /nolog
SQL> connect sys/password as sysdba
SQL> startup
SQL> quit
```

7.6.3 Infrastructure Tier, Database Listener Failure

To check status:
```
ORACLE_HOME/bin/lsnrctl status
```

For **Windows** only, use the Services tool in the Control Panel to check the status

To restart:
```
ORACLE_HOME/bin/lsnrctl start
```

For **Windows** only, use the Services tool in the Control Panel to start the listener

7.6.4 Infrastructure Tier, Oracle Internet Directory Server Process Failure

To check status:
```
ORACLE_HOME/ldap/bin/ldapbind -h
OID_HOST -p OID_PORT
```

For **Windows** only, use the Services tool in the Control Panel to check the status

To restart:
```
ORACLE_HOME/bin/oidctl
server=oidldapd \ configset=0 instance=1 start
```

For **Windows** only, use the Services tool in the Control Panel to start the OID

7.6.5 Infrastructure Tier, Oracle Internet Directory Monitor Process Failure

To check status:
```
ORACLE_HOME/ldap/bin/ldapbind -h OID_HOST -p
OID_PORT
```

To restart:

```
ORACLE_HOME/bin/oidmon start
```

7.6.6 Infrastructure Tier, Enterprise Manager Web Site Failure

To check status:

```
ORACLE_HOME/bin/emctl status
```

For **Windows** only, use the Services tool in the Control Panel to check status

To restart:.

```
ORACLE_HOME/bin/emctl start
```

For **Windows** only, use the Services tool in the Control Panel to start the EM Web site.

7.6.7 Infrastructure Tier, Oracle HTTP Server Process Failure

To check status:

```
ORACLE_HOME/dcm/bin/dcmctl getState
```

To restart:

```
ORACLE_HOME/dcm/bin/dcmctl start -ct ohs -v
```

7.6.8 Infrastructure Tier, OC4J Process Failure

To check status:

```
ORACLE_HOME/dcm/bin/dcmctl getState
```

To restart:

```
ORACLE_HOME/dcm/bin/dcmctl start -ct oc4j -v
```

7.6.9 Infrastructure Tier, OC4J_DAS Instance Failure

To check status:

```
ORACLE_HOME/dcm/bin/dcmctl getState
```

To restart:

```
ORACLE_HOME/dcm/bin/dcmctl start -co OC4J_DAS -v
```

7.6.10 Infrastructure Tier, OPMN Failure

To check status:

```
ORACLE_HOME/opmn/bin/opmnctl status
```

To restart:

```
ORACLE_HOME/opmn/bin/opmnctl startall
```

7.6.11 Infostore Tier, Host Lost, No Data Loss

To restart:
1. Reboot the host.
2. Follow the steps in Section 7.7.5, "Starting the Infostore".

7.6.12 Infostore Tier, Database Instance Failure (Crash)

To check status:
1. Try connecting to the database using SQL*Plus.
2. Check the state as follows:

```
SQL> select status from v$instance;
```

To restart:
```
ORACLE_HOME/bin/sqlplus /nolog
SQL> connect sys/password as sysdba
SQL> startup
SQL> quit
```

7.6.13 Infostore Tier, Database Listener Failure

To check status:
```
ORACLE_HOME/bin/lsnrctl status
```

For **Windows** only, use the Services tool in the Control Panel to check the status

To restart:
```
ORACLE_HOME/bin/lsnrctl start
```

For **Windows** only, use the Services tool in the Control Panel to start the listener

7.6.14 Middle Tier, Host Lost, No Data Loss

To restart:
1. Reboot the host.
2. Follow the steps in Section 7.7.1, "Starting the Middle Tier Instance"

7.6.15 Middle Tier, Enterprise Manager Web Site Failure

To check status:
```
ORACLE_HOME/bin/emctl status
```

To restart:
```
ORACLE_HOME/bin/emctl start
```

7.6.16 Middle Tier, Oracle HTTP Server Process Failure

To check status:

ORACLE_HOME/dcm/bin/dcmctl getState

To restart:

ORACLE_HOME/dcm/bin/dcmctl start -ct ohs -v

7.6.17 Middle Tier, OC4J Process Failure

To check status:

ORACLE_HOME/dcm/bin/dcmctl getState

To restart:

ORACLE_HOME/dcm/bin/dcmctl start -ct oc4j -v

7.6.18 Middle Tier, OC4J_Portal Instance Failure

To check status:

ORACLE_HOME/dcm/bin/dcmctl getState

To restart:

ORACLE_HOME/dcm/bin/dcmctl start -co OC4J_Portal -v

7.6.19 Middle Tier, OPMN failure

To check status:

ORACLE_HOME/opmn/bin/opmnctl status

To restart:

ORACLE_HOME/opmn/bin/opmnctl startall

7.6.20 Middle Tier, Web Cache Failure

To check status:

ORACLE_HOME/bin/webcachectl status

To restart:

ORACLE_HOME/bin/webcachectl start

7.7 Starting and Stopping the Oracle Collaboration Suite Environment

This section contains procedures for starting and stopping middle-tier instances and infrastructures.

7.7.1 Starting the Middle Tier Instance

1. Set the ORACLE_HOME environment variable to the middle-tier Oracle home.

2. For **Unix** only, set the LD_LIBRARY_PATH environment variable to $ORACLE_HOME/lib.

3. Start OPMN, Oracle HTTP Server, and all OC4J instances:

```
ORACLE_HOME/dcm/bin/dcmctl start -v
```

4. Start Oracle Collaboration Suite Web Cache (if configured):

```
ORACLE_HOME/bin/webcachectl start
```

5. Start Discoverer (if configured):

```
ORACLE_HOME/discoverer902/util/startall.sh
```

6. Start Reports (if configured):

```
ORACLE_HOME/bin/rwserver.sh server=name
```

7. Start the Enterprise Manager Web site:

```
ORACLE_HOME/bin/emctl start
```

7.7.2 Stopping the Middle Tier Instance

1. Set the ORACLE_HOME environment variable to the middle-tier Oracle home.

2. Stop the Enterprise Manager Web site:

```
ORACLE_HOME/bin/emctl stop
```

3. Stop Reports (if configured):

```
ORACLE_HOME/bin/rwserver.sh server-name shutdown=yes
```

4. Stop Discoverer (if configured):

```
ORACLE_HOME/discoverer902/util/stopall.sh
```

5. Stop Oracle Collaboration Suite Web Cache (if configured):

```
ORACLE_HOME/bin/webcachectl stop
```

6. Stop Oracle HTTP Server, and all OC4J instances:

```
ORACLE_HOME/dcm/bin/dcmctl stop -v
```

7. Stop OPMN:

```
ORACLE_HOME/opmn/bin/opmnctl stopall
```

7.7.3 Starting the Infrastructure

1. Set the ORACLE_HOME environment variable to the infrastructure Oracle home.

2. Set the ORACLE_SID environment variable to the infrastructure database SID. The default is iasdb.

3. For **Unix** only, set the LD_LIBRARY_PATH environment variable to $ORACLE_HOME/lib.

4. Start the infrastructure database:

```
ORACLE_HOME/bin/lsnrctl start
ORACLE_HOME/bin/sqlplus /nolog
SQL> connect sys/password as sysdba
SQL> startup
```

```
SQL> quit
```

5. Start Oracle Internet Directory.

   ■ Start the Oracle Internet Directory monitor and Wait approximately 30 seconds:

   ```
   ORACLE_HOME/bin/oidmon start
   ```

   ■ Start the Oracle Internet Directory server:

   ```
   ORACLE_HOME/bin/oidctl server=oidldapd configset=0 instance=1 start
   ```

6. Start OPMN, Oracle HTTP Server, and all OC4J instances:

   ```
   ORACLE_HOME/dcm/bin/dcmctl start -v
   ```

7. Start Oracle Collaboration Suite Web Cache (if configured); by default, Web Cache is not configured in an infrastructure:

   ```
   ORACLE_HOME/bin/webcachectl start
   ```

8. Start the Enterprise Manager Web site:

   ```
   ORACLE_HOME/bin/emctl start
   ```

9. Start Intelligent Agent and Oracle Management Server (if configured):

   ```
   ORACLE_HOME/bin/agentctl start agent
   ORACLE_HOME/bin/oemctl start oms
   ```

7.7.4 Stopping the Infrastructure

1. Set the ORACLE_HOME environment variable to the infrastructure Oracle home.

2. Set the ORACLE_SID environment variable to the infrastructure database SID. The default is iasdb.

3. Stop Oracle Management Server and Intelligent Agent (if configured):

   ```
   ORACLE_HOME/bin/oemctl stop oms
   ORACLE_HOME/bin/agentctl stop agent
   ```

4. Stop the Enterprise Manager Web site:

   ```
   ORACLE_HOME/bin/emctl stop
   ```

5. Stop Oracle Collaboration Suite Web Cache (if configured); by default, Web Cache is not configured in an infrastructure:

   ```
   ORACLE_HOME/bin/webcachectl stop
   ```

6. Stop Oracle HTTP Server and all OC4J instances:

   ```
   ORACLE_HOME/dcm/bin/dcmctl stop -v
   ```

7. Stop OPMN:

   ```
   ORACLE_HOME/opmn/bin/opmnctl stopall
   ```

8. Stop Oracle Internet Directory:

   ■ Stop the Oracle Internet Directory server (*n* is the instance number):

```
ORACLE_HOME/bin/oidctl server=oidldapd instance=n stop
```

■ Stop the Oracle Internet Directory monitor (wait approximately 30 seconds):

```
ORACLE_HOME/bin/oidmon stop
```

9. Stop the infrastructure database:

```
ORACLE_HOME/bin/sqlplus /nolog
SQL> connect sys/password as sysdba
SQL> shutdown
SQL> quit

ORACLE_HOME/bin/lsnrctl stop
```

7.7.5 Starting the Infostore

1. Set the ORACLE_HOME environment variable to the infostore Oracle home.

2. Set the ORACLE_SID environment variable to the infostore database SID. The default is ocsdb.

3. For **Unix** only, set the LD_LIBRARY_PATH environment variable to $ORACLE_HOME/lib.

4. Start the database listener:

```
lsnrctl start
```

5. Check the database listener:

```
lsnrctl status
```

6. Start the infostore database:

```
ORACLE_HOME/bin/lsnrctl start
ORACLE_HOME/bin/sqlplus /nolog
SQL> connect sys/password as sysdba
SQL> startup
SQL> quit
```

7.7.6 Stopping the Infostore

1. Set the ORACLE_HOME environment variable to the infostore Oracle home.

2. Set the ORACLE_SID environment variable to the infostore SID. The default is ocsdb.

3. Stop the database listener:

```
lsnrctl stop
```

4. Stop the infostore database:

```
ORACLE_HOME/bin/sqlplus /nolog
SQL> connect sys/password as sysdba
SQL> shutdown
SQL> quit
```

8 Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For additional information, visit the Oracle Accessibility Program Web site at

http://www.oracle.com/accessibility/

Accessibility of Code Examples in Documentation

JAWS, a Windows screen reader, may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, JAWS may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.