

Types of Backups

1. **Full System:** A full system backup stores an image of the entire server disk to a bootable tape. It requires the server be taken offline. A full system backup should be done just prior to system commissioning, and annually thereafter. Restoration of this backup is required should the server hard disk require replacement.
2. **Full Database:** A full database backup may be done with the server either online or offline. Offline backups tend to be simpler to restore. A full database backup should be performed monthly. Restoration of this backup is required should any of the Oracle program files become corrupt.
3. **Database Export:** A database export stores table data only. It may be performed online, but database transactions may not be executed during the export. Database export should be performed weekly. Restoration of this export is required should any of the system data become corrupt or suspect.
4. **Archive Log Export:** Archive log export stores data from the system archive log to tape. It may be performed online. The frequency of this export is dependent on your system activity; weekly is generally appropriate. Restoration of this export is required should a need to access historical data exist.
5. **Images, SIM datafiles, and Applications Backup:** This backup is performed primarily when the Integrated Badging System is installed. Its frequency depends on how often badgeholders are entered into the system. Highly active badging systems should take the backup weekly; less active systems, monthly.

1. Full System Backup

Concept

This procedure creates a complete backup of all programs and files on the server. The created backup tape is bootable; if placed into a system with an empty hard drive, the system will boot from the tape, allowing programs and files to be copied to the disk.

Considerations

- Due to the size of UNIX, this backup will take at least 2 - 2.5 hours even for small EnterpriseSMS systems. Larger systems may take as long as four hours.
- Should your hard disk fail, this backup provides the simplest way to restore the entire system.
- At a minimum, full backups should be taken annually, or whenever changes are made to the operating system environment or devices attached to the system.
- The recovery procedure after a disk failure begins with restoring this backup from tape. Then, subsequent backups of the database are restored, bringing the system to the condition just prior to the last database backup.
- After a full system backup is restored to a server, it can then be updated by restoring backups

of the datafiles taken after the last full backup.

- During full system backup, the server is unavailable. Field controllers cannot update themselves, and OCSs cannot run.

AIX Procedure

1. At a UNIX prompt, log in as sysmgr. Enter:

```
% team_stop
% z_clean all
% dbshut
% lsnrctl stop
```

2. Place a tape in the tape drive, and log into the system as root . Enter:

```
# smit &
```

3. When the smit interface appears, click on *System Storage Management*, then *System Backup Manager*, then *Backup the System*. Fill in the form according to the options below.

- In *Backup DEVICE or FILE*, click *List*, and select the name of the system tape drive. This is usually /dev/rmt1.
- For *Create MAP files*, enter no.
- For *EXCLUDE files*, enter no.
- For *Make BOOTABLE backup*, enter yes.
- For *EXPAND /tmp* if needed, enter yes.
- For *Number of BLOCKS to write in single output*, leaveblank.

4. Click *OK*. The system will create an image backup to the backup device.

5. When finished, restart the system:

```
% dbstart
% lsnrctl start
% team_start amm
% team_start sim
```

2. Full Database Backup

Concept

After a full system backup is taken, the administrator takes database backups on a regular basis (daily in highly active systems, weekly in more static systems). If necessary, the latest backup is added to the full system backup to bring the system back to its most recent condition.

The decision to do *offline* or *online* backups is left to the system administrator. Offline backups are simpler and easier to restore, but requires that OCS's and system databases be down during backup. Online backups are more complex, and require more free workspace on disk. However, they permit 24x7 operation.

Offline Backup Procedure

1. Insure all users and client stations are logged off. At the UNIX prompt, enter the following:

```
% team_stop
```

2. After the system processes shut down, enter the following:

```
% dbshut
```

3. After the database shuts down, enter the following:

```
% lsnrctl stop
```

4. Log in using the root password, then change to the oracle home directory:

```
% su  
root's password:  
% cd $ORACLE_HOME/dbs
```

5. Place a tape into the server tape drive. Enter the following. If necessary, continue typing past the edge of the screen; the command will automatically wrap.

```
% tar -cvf /dev/rmt0 /usr/oracle/dbs/* /ims/* /usr/sim/bin/dat/*
```

6. Restart the system:

```
% lsnrctl start  
% dbstart  
% team_start
```

Online Backup Procedures

Concept

The online backup procedure first takes the tablespaces (containing the actual data tables) to be backed up offline. When a tablespace goes offline, the last record in its tables are checkpointed, while subsequent transactions are posted to a *Redo Log*. The tablespace is then brought back online, closing the redo log. The tablespace and its redo log are then copied to the backup volume. Should the backup be restored, the backed up tablespace is copied to disk, and the transactions in its redo log are applied to the database.

Procedure: Checking Database Operation Mode

1. This procedure assumes you are running your database in *archive log* mode. To check the mode you are running in, enter the following:

```
% sqlplus sys/<password>  
% select log_mode from sys.v$database;
```

2. If you are not running in archive log mode, change the mode as follows:

```
% cd /usr/oracle/dbs  
% su oracle/<password>  
% vi configamg.ora
```

3. Edit the log_archive_dest parameter as follows:

```
> log_archive_dest = /usr/oracle/dbs/arch/arch%S.log
```

4. Exit vi and enter:

```
% vi initamg.ora
```

5. Edit the following parameters in the file:

```
> log_archive_start = true  
> log_archive_format = arch%S.log
```

6. Exit vi and enter:

```
% mkdir /usr/oracle/dbs/arch
```

7. Shutdown the database then start it in archivelog mode:

```
% su sysmgr/< password>  
% dbshut  
% sqldba mode=line  
SQLDBA> connect internal  
SQLDBA> startup mount amg;  
SQLDBA> alter database amg archivelog;  
SQLDBA> alter database amg open;
```

8. Exit sqldba. Stop and restart the database to verify that archivelog mode is in effect:

```
% dbshut  
% dbstart  
% sqlplus sys/<password>  
% select log_mode from sys.v$database;
```

9. Start Server Manager, select *Instance*, then *Initialization*. Verify that the archivelog settings are correct:

```
log_archive_start = TRUE  
log_destination = /usr/oracle/dbs/arch/arch%S.log
```

Procedure: Online Backup

1. Insure all users and client stations are logged off. Start the Server Manager from the popup menu.
2. Tab on *Recovery*, then *Backup*.
3. Singleclick on ACC_TSP. Execute BACKUP-START ONLINE BACKUP. The *Status* of the tablespace will change to *Ready for Backup*.
4. Repeat Step (3) for each of the tablespaces displayed.
5. Tab on *Redo Logs*. Click on the line marked *Group 2*.
6. Execute REDO-FORCE CHECKPOINT, then REDO-SWITCH LOGFILE. The group's status of 2 will change to *Inactive*. At this point, the status of group 1 should be *Current*. Note the current redo logfile's *Sequence #*. All archive logs with sequence numbers less than that of the *Current* logfile will be archived to tape along with the tablespaces.
7. Copy the offline tablespaces to the backup media (e.g., tape) by entering the following in an

open window:

```
% su
root's password:
# cd /usr/oracle/dbs
# tar cvf /dev/rmt0 /usr/oracle/dbs/* /ims/* /usr/nim/bin/dat/*
```

8. Return to Server Manager and tab on *Backup*. Click ACC_TSP, and execute BACKUP-END ONLINE BACKUP. This will close the redo logs and return the tablespace to normal process.

9. Repeat Step (9) for each of the tablespaces displayed.

10. Copy the redo logs to the backup tape by entering the following:

```
# cd arch
# tar cvf /dev/rmt0 /usr/oracle/dbs/* /ims/* /usr/nim/bin/dat/*
```

11. Remove the redo log files by entering:

```
# cd /usr/oracle/dbs/arch
# ls -al arch*.log
# rm arch%S*.log
# exit
```

12. Remove the backup tape and close the UNIX window.

3. Archive Log Export

Concept

EnterpriseSMS keeps two logs of system activities. The *Event Log* (event_log_tbl) receives event activity from the system in real time. The event log is online at all times. Each day at a time designated in the EVENT-SCHEDULED EVENTS form (by default 0100 hours) the SQL script SYS1000S.SQL (located in the directory /usr/amm/runsql) runs. This script copies aged records (by default those older than 7 days) from the *Event Log* to the Archive Log (archlog_tbl) and deletes copied records from the event log. The event log, therefore, is maintained in an approximately fixed size. It is therefore never necessary (or desirable) to export the event log.

The logs have maximum sizes that are set in the amm_mon file by the logtbl_proc entry (defaults 50,000 records event log, 100,000 records archive log). Alarms are posted to the Operator Command Station when the archive log reaches 70%, 80% and 90% full.

Proper Use

- Set a policy for determining how much information the archive log will be permitted to contain before it is *truncated*. Truncating the archive log deletes all records from it, but leaves its table structure intact, ready to receive new records when the next transfer from the event log occurs.
- The archive log table should be truncated on a regular interval. This interval should be determined to avoid 80% full alarms from appearing on the OCS.
- If such alarms regularly appear before the end of the determined interval, truncate the table more often. If this recommendation prevents sufficient history from being kept online, adjust the number of records permitted in the table in the amm_mon file.

- Always export the archive log to tape before truncating the table.
- Export your archive log weekly. Properly label and date the export tape and store in a secure location according to your facility's MIS procedures. The label should contain the date range between which records in the exported log were generated (7 days prior to the current date, and the date the log was last truncated).
- Export and truncate the archive log according to your determined interval. Properly label and date the export tape and store in a secure location according to your facility's MIS procedures. The label should contain the date range between which records in the exported log were generated (7 days prior to the current date, and the date the log was last truncated).
- After truncating the table, previous export tapes made between the last two truncations may be reused.

Procedure

1. Point to the system background, click and hold the right mouse button down to display the system shortcut menu. Select *New Window* from the menu.
2. Log in as sysmgr. Enter:
 - > ESMS.backup
3. Select *Export Archive Log to Tape*.
4. When prompted for a password, enter ics. Press *Enter*.
5. Select the identifier of the tape drive to be used for backup and press *Enter*. The system responds:
 - . . exporting table archlog_tbl
6. When finished, remove and store the tape.

