

NN10031-111

Succession Multimedia Communications Portfolio

MCP Database Module

Basics

Standard MCP 1.1 FP1 (02.02) April 2003



Overview

The Database Module uses the Oracle Enterprise Manager to configure, administer, and monitor provisioned subscriber and configuration data.

How this guide is organized

This document provides an overview of Database Module architecture, including data replication and data transfer concepts. The following principal tasks performed with the Database Module are also documented.

- Configuring the Oracle Enterprise Manager to perform backups, observer accounts and email notification. See “Oracle Enterprise Manager configuration” on page 7 and “Configuration management” on page 43.
- Administering backup and recovery of data, resolving replication errors, resynchronizing databases, and managing disk space. See “Database administration” on page 7 and “Security and Administration” on page 69.
- Monitoring faults related to backups, events, and replication jobs, as well as monitoring alert logs and trace files and disk usage and generating reports. See “Fault management” on page 8 and “Fault management” on page 17.

Required hardware, software, tools and utilities, and OAM&P strategy are explained later in this chapter. See “MCP hardware” on page 10.

Other Database Module concepts and tasks explained are

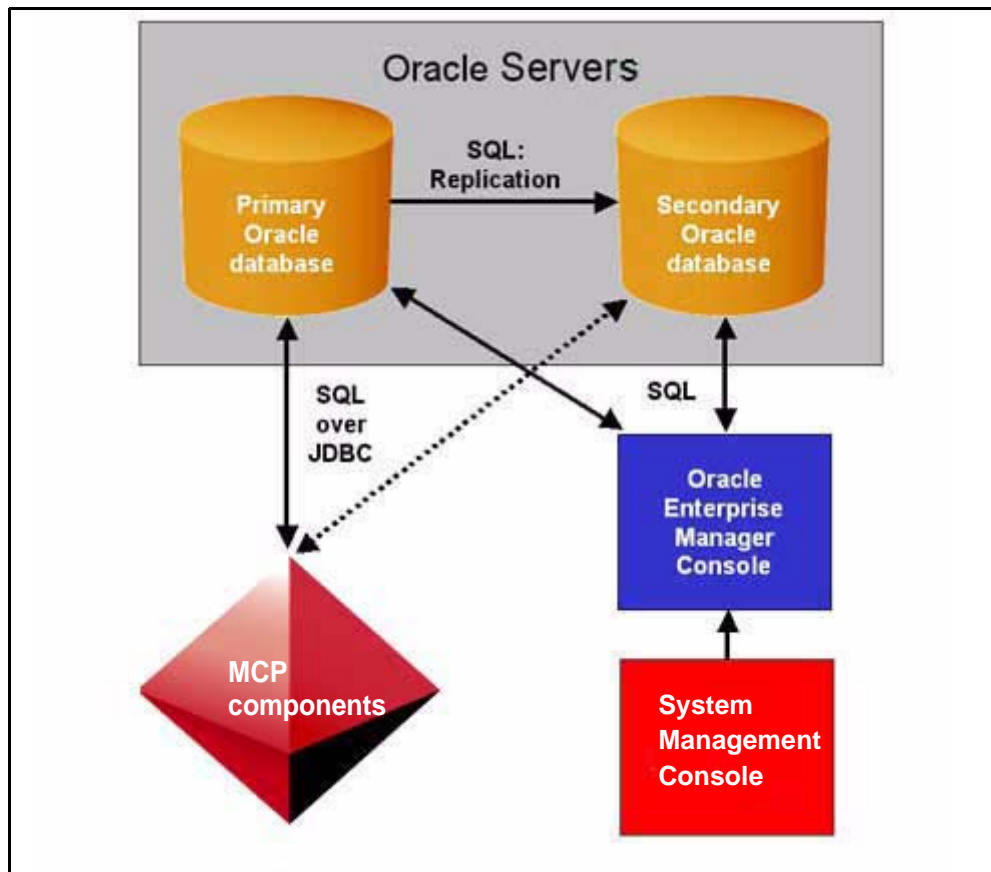
- Upgrades: Maintenance upgrades required between major product releases. See “Upgrades” on page 13.
- Performance management: Where to observe logs and alarms and how database failover works. See “Performance management” on page 67.

Architecture

As shown in Figure 1, the Database Module consists of Oracle Servers having a primary database and a replicated secondary database managed from the Oracle Enterprise Manager (OEM) Console. The Oracle databases operate in replicated mode and applications and components normally send and receive data directly to and from the primary database.

Monitoring logs, alarms, and operational measurements, OEM login, and maintenance updates are done from the System Management Console.

Figure 1 Database Module architecture normal operation



Note: Nortel Networks recommends that you back up the database daily whether it is a redundant configuration or not. If there is no redundancy in the network, there is no replication process, so backup of the data is even more important.

For information about the communication protocols and interactions between the Database Module and network components, see Figure 2, “SQL over JDBC,” on page 11.

Each database includes replicated objects and non-replicated objects. Tables are the only objects that are replicated. Non-replicated objects include stored procedures, functions, and views.

Minimal, redundant, and variable server configurations are supported in enterprise deployments. Redundant and variable configurations have replicated databases. Minimal configurations have a single database.

Data replication

During normal operation, applications send data to the primary database, which is then stored in tables. The Oracle Server uses a process called master-master data replication to constantly transfer changed data from the primary database to the secondary database. See “Data transfer” on page 7.

Consequently, in the unlikely event of failure of the primary database, the secondary database should always contain a copy of the data. See “Fault management” on page 8.

For applications, the secondary database operates in limited write mode only, which means that it is read only except for registrations. See Table 1, “Database operational states,” on page 6 and “Fault management” on page 17.

ATTENTION

Database Module deployment creates or updates both replicated objects (database tables) and non-replicated objects (stored procedures, functions, and views) on both databases.

The Database Module replication environment has the states of operation identified in Table 1, “Database operational states,” on page 6. The primary database ordinarily operates in the normal state,

while the secondary database operates in a limited write state at all times.

Table 1 Database operational states

Database states	Description
Normal (Primary database)	Fully writable for applications. Inserts, updates, or deletions are permitted to the primary database. The Oracle Server continuously transfers changed data to the secondary database.
Limited write (Secondary database)	<p>Read only for applications with the exception of registrations (inserts, updates, or deletions).</p> <p>In the unlikely event of failure of the primary database, applications failover to the secondary database. During failover, applications can read and have limited write access to the secondary database. The failover state continues only until the primary database returns to service.</p> <p>Note: The secondary database operates in a limited write state for applications but is always fully writable for Oracle replication processes.</p>
Quiesced (maintenance mode)	<p>No writes are permitted to either database.</p> <p>When the database is quiesced, applications can only query the database and cannot insert, update, or delete database records.</p> <p>Replicated databases automatically enter this state whenever changes are being made to the replication environment, including modifying replication objects and synchronizing the two databases.</p>

Data transfer

When data transactions occur, updates to the primary database are queued for transfer to the secondary database. Similarly, changes made to the secondary database are queued for transfer to the primary database. See “Database failover” on page 19.

The data transfer process between the primary and secondary databases is managed by push and purge jobs, described as follows:

- **Push jobs:** When push jobs execute, they reassign all transactions in the queue to the other master site. Push jobs are scheduled every 30 seconds.
- **Purge jobs:** When purge jobs execute, they purge or delete all transactions in the queue that have been transferred to the other master site. Purge jobs are scheduled every 10 minutes.

Note: The frequency of push and purge jobs is based on optimal values established during testing.

Oracle Enterprise Manager configuration

Oracle Enterprise Manager (OEM) configuration is done from the OEM Console. Tasks include OEM Console login, configuring the databases for backups, configuring the SYSMAN user to receive email notifications, and configuring OBSERVER accounts. See “Configuration management” on page 43.

Configuration is performed during installation after the Database Module has been deployed. See “Application database connection configuration” on page 57.

Database administration

Database Module administration consists of backup, recovery, resynchronization, and disk space management. See “Security and Administration” on page 69.

Database backups

In addition to the redundancy provided by Oracle replication explained earlier in this chapter, the Database Module supports taking backups using the OEM Console.

The export backup method is recommended over Recovery Manager (RMAN) backups.

For details, see “Database backups” on page 71.

Database recovery

Recovery restores a database to its original state after a failure. See “Database recovery” on page 84.

Manage replication transaction errors

The OEM Console provides tools for resolving replication errors, should they occur. Replication errors can result from a lack of available space in a table targeted for an update or other unresolved replication conflicts.

For additional information, see “Resolving replication errors” on page 89.

Resynchronization

Replicated databases should always be in synchronization. In the unlikely event that changes made to one database are not successfully propagated to the other, the two databases become out of synchronization and must be manually resynchronized. See “Resynchronization” on page 92.

Disk space management

A script called **optimize_dbSPACE** drops and recreates Database Module indexes to reduce disk space usage. See “Disk space management” on page 93.

Fault management

Use the OEM Console to monitor and respond to Database Module faults in the categories listed in this section. Note the recommended frequency for each task.

- **Replication:** Replication jobs ensure that the primary and secondary databases remain synchronized.
Therefore it is critical that you use the OEM Console to monitor replication jobs once every 24 hours to ensure the databases remain synchronized.
See “Monitor replication jobs” on page 27 and “Resolving replication errors” on page 89.
- **Backups:** Once backup jobs have been scheduled using the Oracle Enterprise Manager (OEM) Console, the system backs up the database at predefined periods and sends a status email to the operator.

It is recommended that you monitor backup status to ensure the backup was successful. See “Monitoring backups” on page 20.

- **Events:** Database events are processed by the Oracle Enterprise Manager and alerts are generated when specified error thresholds are reached. Monitor events as required and respond to alerts as appropriate. See “Event monitoring” on page 23.
- **Alert logs and trace files:** When an Oracle process detects an internal error, it dumps information about the error into a trace file. Each Database Module also has an alert file. The alert file is a chronological log of messages and errors, such as all internal errors, block corruption errors, and deadlock errors. See “Alert log and trace file monitoring” on page 35.
- **Tablespaces:** Nortel Networks recommends that you regularly monitor tablespaces and ensure that they do not run out of disk space.
To monitor tablespace sizes and disk space usage or set thresholds for generating alert logs and trace files, use either the System Management Console (Oracle Monitor Application) or the OEM Console.
- **Reports:** The OEM Console can generate reports about configuration, status, events, and backup jobs as required. See “Reports” on page 37.
- **Oracle Monitoring Application:** See “Tools and utilities” on page 10.

Failover

Failover occurs when an application identifies a problem with the primary database. During a failover, applications begin using the secondary database. Because the two databases are replicated, they contain consistent data and the query information is automatically supplied from the secondary database. See “Fault management” on page 17.


Security

The Database Module uses Oracle database technology to ensure confidentiality, integrity, and availability of data. The Database Module is also protected by user authentication and network firewalls configured in a network architecture.

For additional information, see *MCP Basics* and “Security” on page 95.

MCP hardware

The Database Module is deployed on a pair of Sun Netra t1400/1405s servers configured in an Oracle master-master replication mode for redundancy.

Hardware	Details
<p>Primary and Secondary Database servers</p> 	<p>Sun Netra t 1400 or Sun Netra t 1405 with the following hardware features:</p> <ul style="list-style-type: none"> - 4 440 Mhz CPUs - 4 GB RAM - 4 36.4-GB hard disks - 10x Internal DVD-ROM drive - 20-GB 4mm DDS-4 Internal tape drive - 1 Quad Fast Ethernet (QFE) PCI card - 1400 server is DC powered; 1405 server is AC powered

Note: Minimal configurations use a single database, and thus only one server is required.

Tools and utilities

The following tools are used to configure and maintain the Database Module:

- **System Management Console:** Launches the OEM Console and Oracle Monitoring Application. Provides log and alarm information. For details, see *MCP System Management Console Basics*.
- **Oracle Enterprise Manager (OEM) Console:** Used by the database administrator for backup and recovery and database fault management.
For details, see “Security and Administration” on page 69 and “Fault management” on page 17.
- **Oracle Monitoring Application:** Gathers operational status of the database and sends alarms and operational measurements (OMs) to the System Management Console. The tool uses Oracle SNMP agents to gather information about disk and tablespace utilization, and other information.
For details, see “The Oracle Monitor component” on page 41.

Network interfaces and protocols

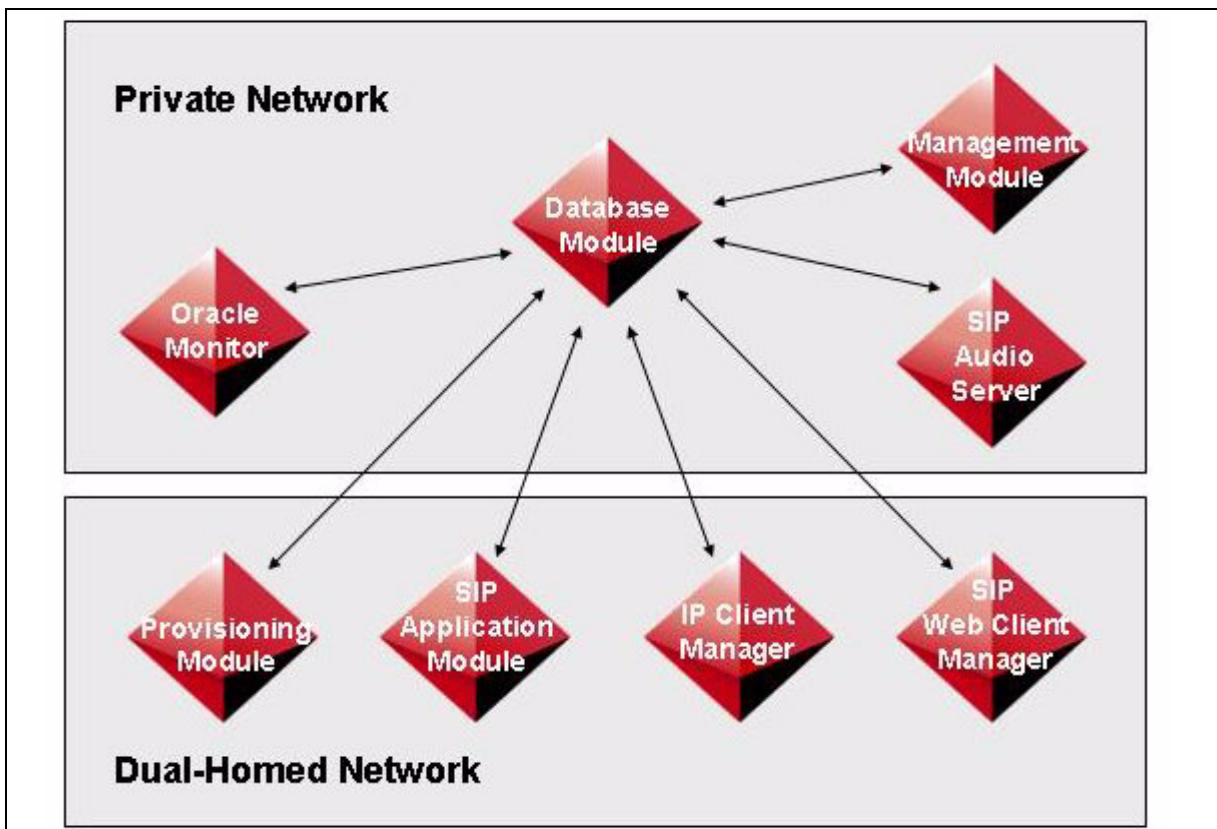
User interfaces which access the Database Module are:

- **SQL over JDBC:** The Database Module communicates with network components using Structured Query Language (SQL) over Java Database Connection (JDBC). See Figure 2, “SQL over JDBC,” on page 11 and Figure 1, “Database Module architecture normal operation,” on page 4.

As shown in Figure 2, all communication between applications and the Database is by SQL over JDBC.

Note: The SIP Audio Server connects to the Database Module during initialization only. There is no interaction between the SIP Audio Server and Database Module after initialization.

Figure 2 SQL over JDBC



- **SNMP:** The Oracle Monitoring Application uses a Simple Network Management Protocol (SNMP) agent running on the Database Module to gather database state information.

Note: The OracleMonitor is a software application designed/implemented by Nortel Networks and deployed from

the System Management Console. The OracleMonitor extracts (using SNMP *gets* and SQL queries) information concerning the health of the database. This information is then transformed into alarms/logs/OMs, allowing the data to be viewed from the System Management Console Alarm/Log/OM browsers.

OAM&P strategy

Offline data migration between releases and maintenance updates are supported. See “Upgrades” on page 13.

Database backup, recovery, and resynchronization are also supported. See “Security and Administration” on page 69.

Legal note

All basic operations of the Oracle programs which are embedded in this Nortel Networks application, including but not limited to database management operations, must be managed from within this application.



Upgrades

Strategy

The following deployment tasks related to the Database Module are performed by your next level of support:

- Adds and configures the server(s) hosting the Database Module
- Installs Oracle
- Deploys the Database Module software onto the server(s)

Offline migration

Off-line migration of data between releases enables upgrading the Database Module from one release to the next without loss of data.

Once the Database Module is upgraded to a new release, it can be updated or reverted to previous maintenance releases.

Prior to an upgrade, the system automatically creates a backup of the existing database, assigning a backup name that contains the release name. That backup is then available if necessary to restore the database to an earlier release.

Task flows

Refer to Table 2, “Upgrade task flows” for a list of upgrade procedures contained in this section.

Table 2 Upgrade task flows

Topic	Sub-topic	Procedure
“Database Module updates”	Deployment	“Updating a Database Module” on page 14
	Reverting	“Reverting to a previous version of the database” on page 15

Tools and utilities

Database Module maintenance updates are deployed from the System Management Console. For details, see *MCP System Management Console Basics*.

Database Module updates

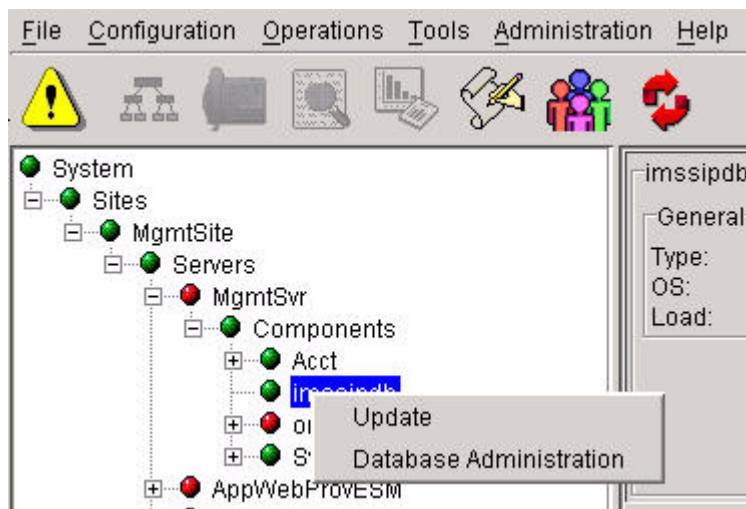
Database Module maintenance updates include database schema files, stored procedures, and backup and recovery scripts. Full upgrades are done by your next level of support.

Maintenance updates can be done as explained in the following procedure.

Updating a Database Module

From the System Management Console

- 1 In the System tree, right-click the database version to be updated as shown.



- 2 From the flyout menu, click **Update**.
The **Load List dialog box** opens with list of available maintenance releases.
- 3 Select the required database version and click **OK** to install it.
The deployment tool copies the appropriate database scripts onto the database server.

Reverting to a previous version of the database

If you want to revert to a previous version of the database, you must redeploy a previous version of the database over the current database.

In such a scenario, the user is first prompted to confirm that they want to revert to a previous version of the database. The user is then warned that doing so removes data gathered since the previous update. An older version of the database is then restored. See “Database backups” on page 71.



CAUTION

When the database is replaced by a backup, any newly provisioned subscriber or configuration data is lost. The restored data will be exactly as it was before the newer release was deployed.

Contact your next level of support for assistance prior to reverting the database to a previous version.

Undeploying a database

A database should never be undeployed. As explained in the previous section, if you need to revert to a previous version of the database, you must redeploy a previous version.



Fault management

Strategy

Database Module fault management consists of monitoring and responding to logs and alarms from the Oracle Enterprise Manager (OEM) Console and the System Management Console. See *MCP System Management Console Basics*.

The Database Module is built on an Oracle database and provides high availability using Oracle Replication to a secondary database on a separate server. As updates are applied to the primary database, they are transferred to the secondary (replicated) database.

To provide additional redundancy, databases should be backed up on a regular basis. For backup and recovery procedures, see “Security and Administration” on page 69.



CAUTION

Nortel Networks recommends that the primary and secondary databases and external backup media be maintained in separate geographic locations to prevent data loss in case of natural disaster, security breach, or other unforeseen event.

Task flows

Table 3 outlines Database Module performance management tasks.

Table 3 Performance management task flows

Topic	Subtopic	Procedure
Database monitoring	Backups	“Monitoring backups” on page 20
	Events	“Monitoring events” on page 24
	Replication	“Monitoring replication” on page 28
		“Monitoring registration deletions” on page 31
	Alert logs and trace files	“Monitoring alert logs and trace files” on page 35
	Disk usage	“Monitoring disk usage” on page 36
	Alarm monitoring	“Monitoring alarms” on page 34
	Reports	“Generating reports” on page 37
	Oracle Monitoring Application	“Querying or modifying Oracle Monitor configuration properties” on page 59

Tools and utilities

Use the following tools to perform Database Module fault monitoring tasks:

- Oracle Enterprise Manager (OEM) Console: Used by the database administrator for backup and recovery and database fault management.

For details, see “Security and Administration” on page 69.

- System Management Console: Launches the OEM Console and Oracle Monitoring Application. Provides log and alarm information. For details, see MCP System Management Console Basics.
- Oracle Monitoring Application: Gathers operational status of the database and sends alarms and operational measurements (OMs) to the System Management Console. The tool uses Oracle SNMP agents to gather information about disk and tablespace utilization, and other information.

For details, see “The Oracle Monitor component” on page 41.

Database failover

In the unlikely event of a failure of the primary database, application queries are redirected to, that is, “failover” to the secondary database.

During a failover only registration data can be written to the secondary database and application components periodically attempt to access the primary database. Once the primary database returns to service, all data processing reverts to the primary database.

All applications access and update data via request/response transactions. If the primary database does not respond to a request, the initiator of the request does the following:

- Raises an alarm indicating a problem with the database
- Switches over to the secondary database and reinitiates the request

ATTENTION

A minor alarm is raised when applications are connected to the primary database and the connection to the secondary database fails.

For information about database backup and recovery, resynchronization, replication, and optimization, see “Security and Administration” on page 69.

Database monitoring from the Oracle Enterprise Manager Console

To launch the OEM Console, see “Logging in to the OEM Console” on page 45.

Monitoring backups

When a database backup starts, an email is sent to the administrator. Another email is sent when the job completes. The status of completion of the job is included in that email.

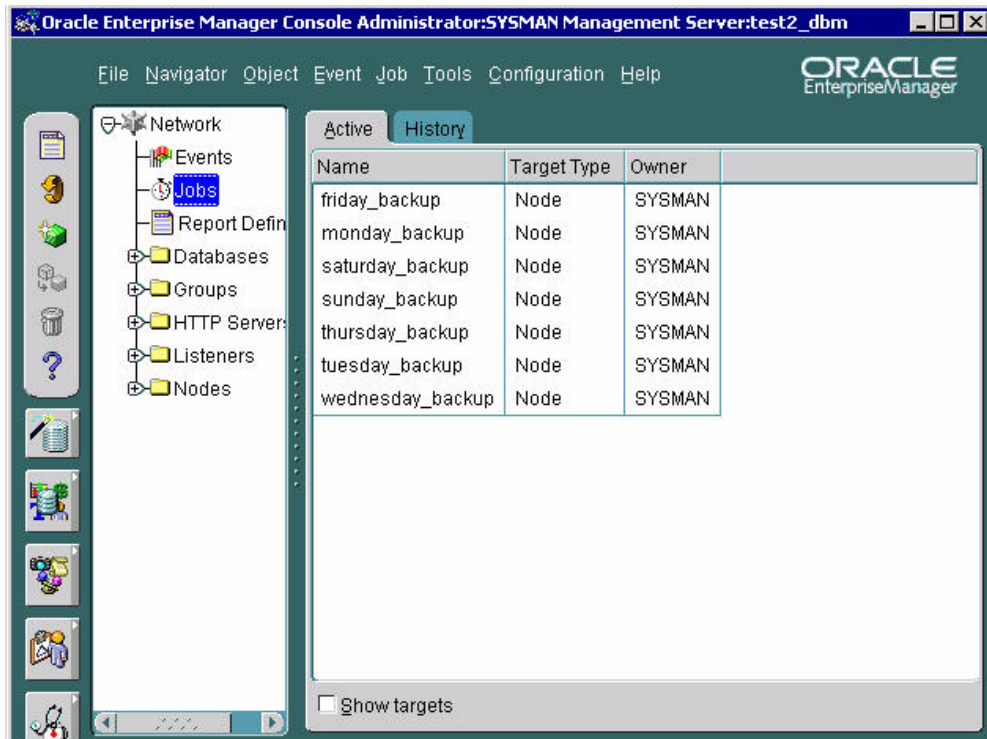
In addition to email notification, the administrator can view the output log of the backup job, as explained in “Monitoring events” on page 24.

Also use this procedure to debug failed database backup jobs.

For login instructions, see “OEM Console login” on page 45.

From the OEM Console

- 1 From the **Network** tree, select **Jobs**.

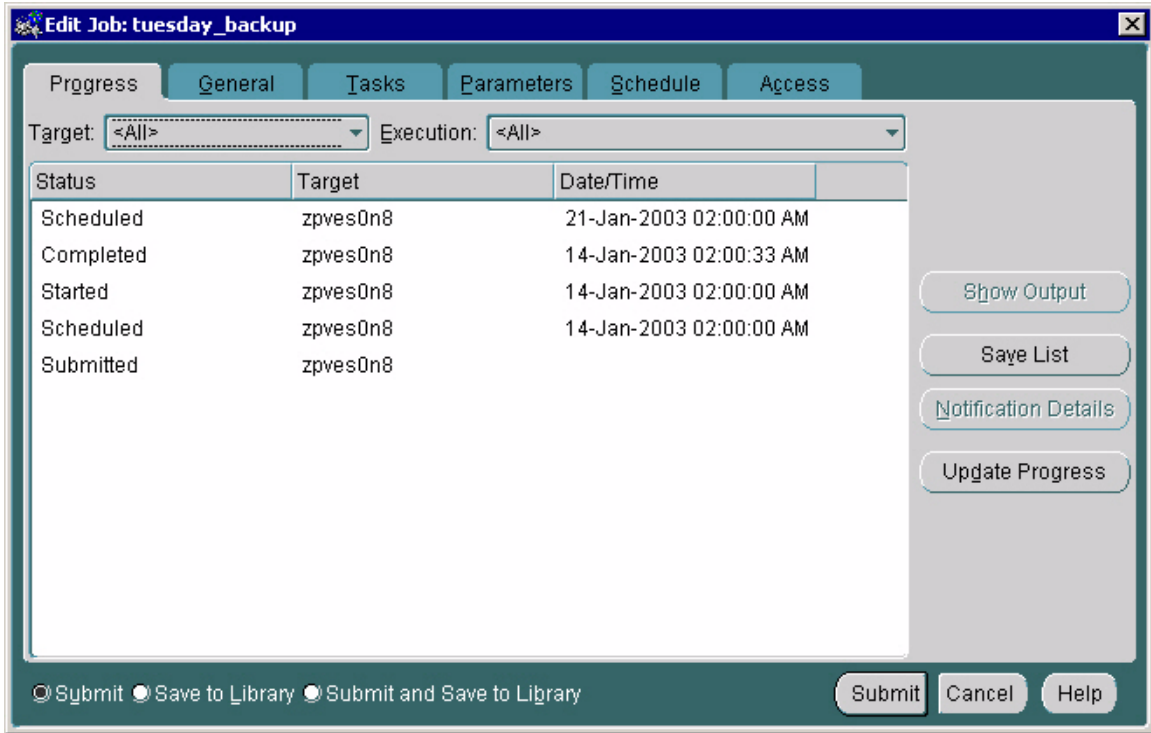


The **Jobs > Active** pane displays the list of active backup jobs that have been scheduled.

- 2 Select the **History** tab.

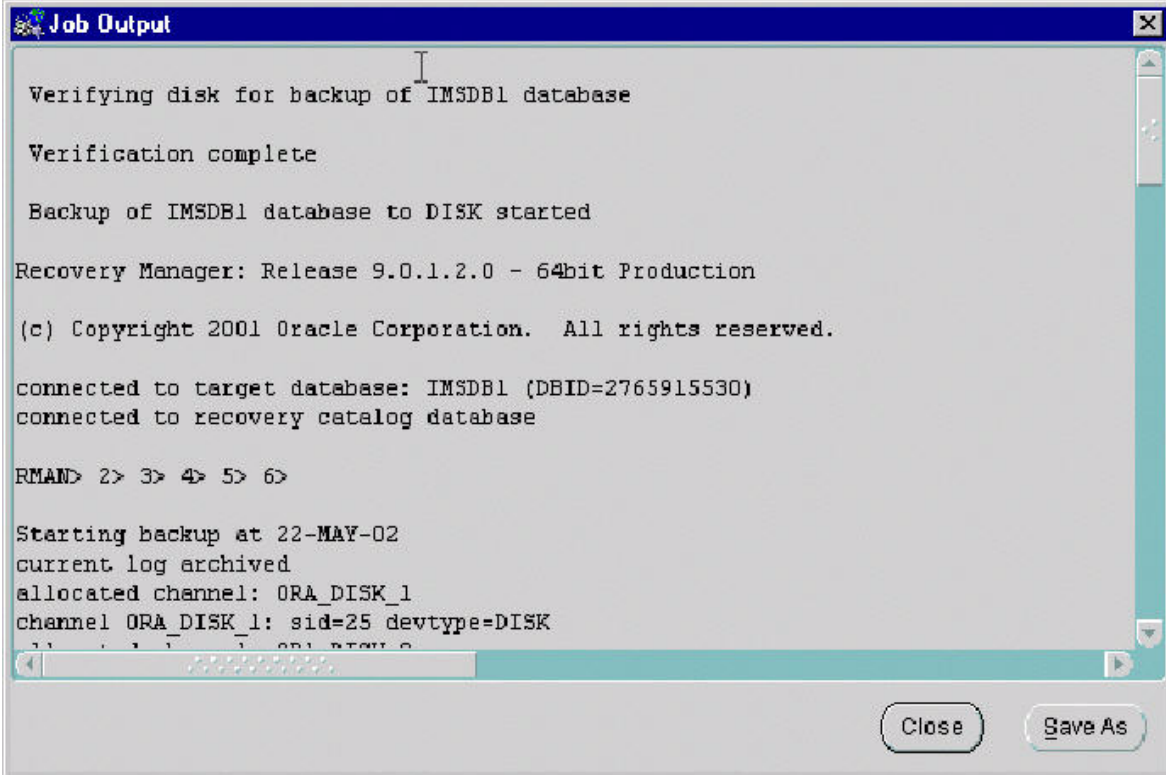
The **Jobs > History** pane shows the list of completed jobs.

- 3 In the **History** pane, double-click the appropriate job to display its properties.
The **Edit Job > Progress** window opens, showing when the job started and completed.



- 4 To see the output of the job, select the a **Completed** or **Failed** job and click **Show Output**.

The **Job Output** window opens, displaying the job status, target node, and the date and time the job executed.



```
Job Output
Verifying disk for backup of IMSDB1 database
Verification complete
Backup of IMSDB1 database to DISK started
Recovery Manager: Release 9.0.1.2.0 - 64bit Production
(c) Copyright 2001 Oracle Corporation. All rights reserved.
connected to target database: IMSDB1 (DBID=2765915530)
connected to recovery catalog database
RMAN> 2> 3> 4> 5> 6>
Starting backup at 22-MAY-02
current log archived
allocated channel: ORA_DISK_1
channel ORA_DISK_1: sid=25 devtype=DISK
```

Event monitoring

When a registered event exceeds a specified threshold, an alert displays on the OEM Console and an email is sent to the administrator. Alerts have progressively higher severity levels as shown in the following table.

Alert State	Icon description	Alert description
Critical	Red flag	A red flag would indicate a critical alert.
Warning	Yellow flag	A warning threshold has been reached.
Error State	Yellow hexagon with an exclamation point	An error state indicates there is a problem with the evaluation of the event condition, as opposed to a threshold being met.
Event Cleared	Green flag	The event has been cleared. Example, when the database goes down and comes back up.
Unknown	Gray Flag	A gray flag represents an "unknown" state where it is not possible for the Oracle Enterprise Manager to ascertain the event status because the node is unreachable or the Intelligent Agent is not available.

Monitoring events

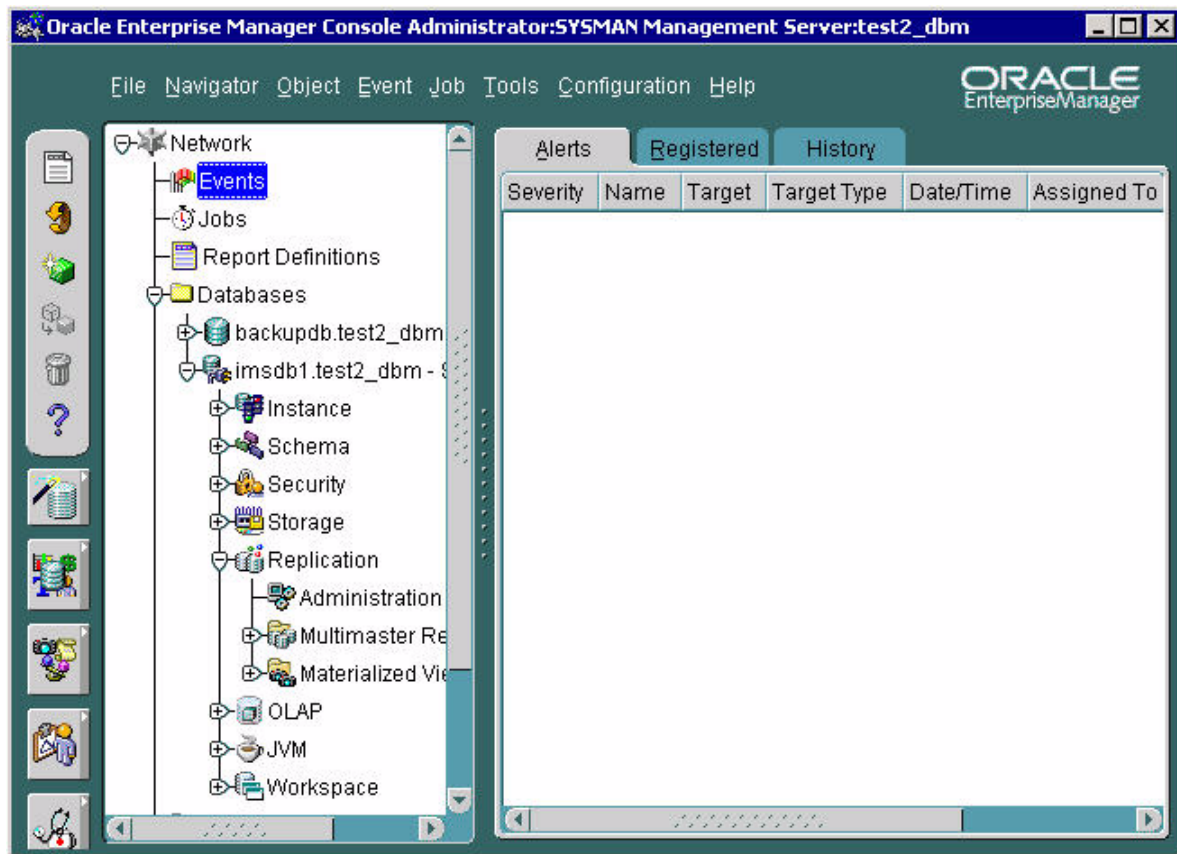
Monitor and respond to events as required to ensure smooth database operation. See “Event monitoring” on page 23.

For login instructions, see “OEM Console login” on page 45.

From the OEM Console

- 1 From the **Network** tree, select **Events**.

The **Network Events > Alerts** pane opens, listing all current alerts.



- 2 Click the **Registered** tab to list all registered alerts.
- 3 Click the **History** tab to list all cleared alerts.

Table 4 lists database event types and descriptions.

Table 4 Database events

Events	Type	Description
Alert	Fault	New errors were shown in alert.log file.
Archiver Hung	Fault	The archive process is hung.
Broken Jobs	Fault	Broken jobs exist.
Database UpDown	Fault	The database was shutdown.
Data Block Corruption	Fault	A corrupted block was detected.
Deferred Transactions	Fault	The number of deferred transactions is too high (only in replicated systems).
Error Transactions	Fault	The number of error transactions is too high (only in replicated systems).
Failed Jobs	Fault	A job has failed to execute.
Datafile Limit	Resource	The maximum datafile limit is being approached.
Process Limit	Resource	Maximum process limit has been reached.
Session Limit	Resource	The maximum session limit is being approached.
Alert File Large	Space	The alert file is too large.

Table 4 Database events

Events	Type	Description
Archive full	Space	The archive device is full.
Dump Full	Space	The dump destination is full.
Index Rebuild	Space	Some indexes may benefit from being rebuilt.
Maximum Extents	Space	The segments maximum limit is being approached.
Tablespace Full	Space	A tablespace is full.

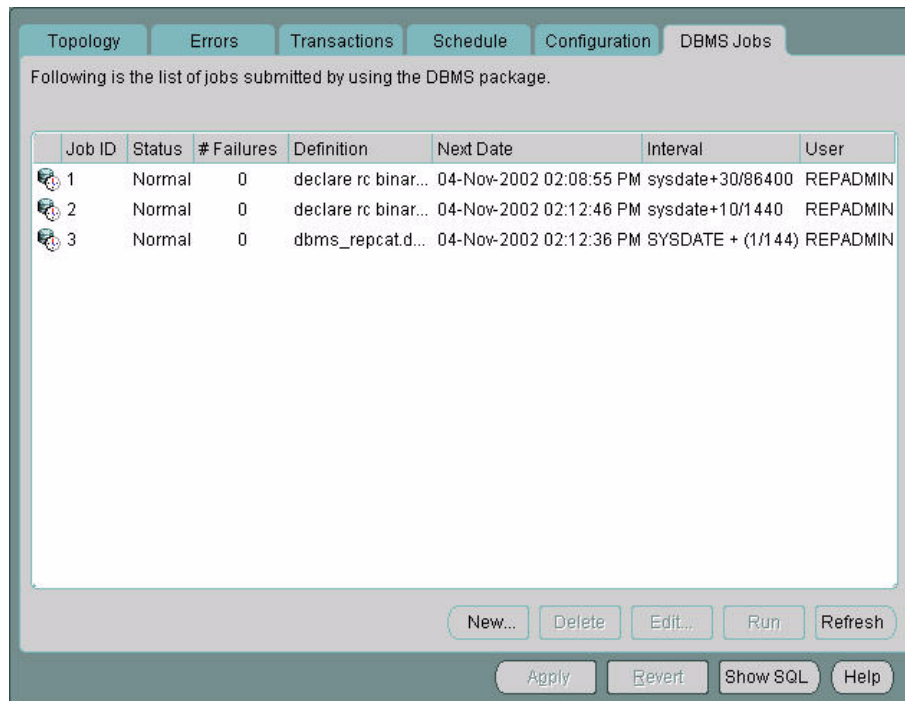
Monitor replication jobs

The **DBMS Jobs** tab lists all the active jobs in the system. In the **DBMS Jobs** screen shown in Figure 3, three normal jobs are listed.

If a job fails to execute, details of the failure display in the **# Failures** column. Each replication job retries 16 times before it is marked broken.

If a replication job is broken, then the operator must correct and reschedule the job. See “Monitor replication jobs” on page 27.

Figure 3 OEM Replication Administration DBMS jobs window



Job ID	Status	# Failures	Definition	Next Date	Interval	User
1	Normal	0	declare rc binar...	04-Nov-2002 02:08:55 PM	sysdate+30/86400	REPADMIN
2	Normal	0	declare rc binar...	04-Nov-2002 02:12:46 PM	sysdate+10/1440	REPADMIN
3	Normal	0	dbms_repcat.d...	04-Nov-2002 02:12:36 PM	SYSDATE + (1/144)	REPADMIN



CAUTION

After a restart, there is a higher probability that replication jobs may be broken. Therefore, be sure to monitor jobs closely after any restart.

Monitoring replication

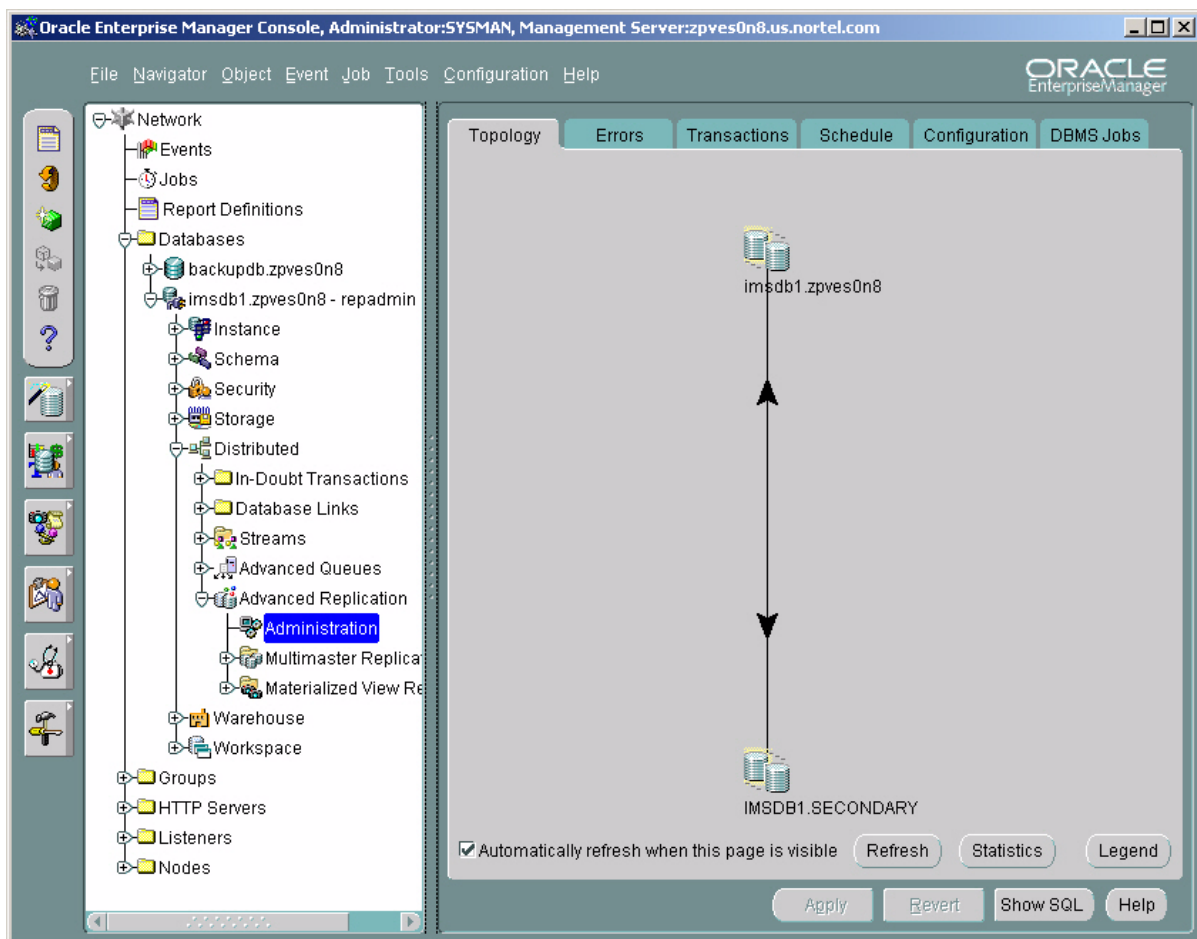
Oracle replication should be monitored regularly for conflict alerts. For details about replication, see “Data replication” on page 5.

For login instructions, see “OEM Console login” on page 45.

From the OEM Console

- 1 Login as **sysman**.
- 2 From the **Network** tree, select the database you want to monitor and expand the tree.
- 3 Select **Distributed > Advanced Replication > Administration**.

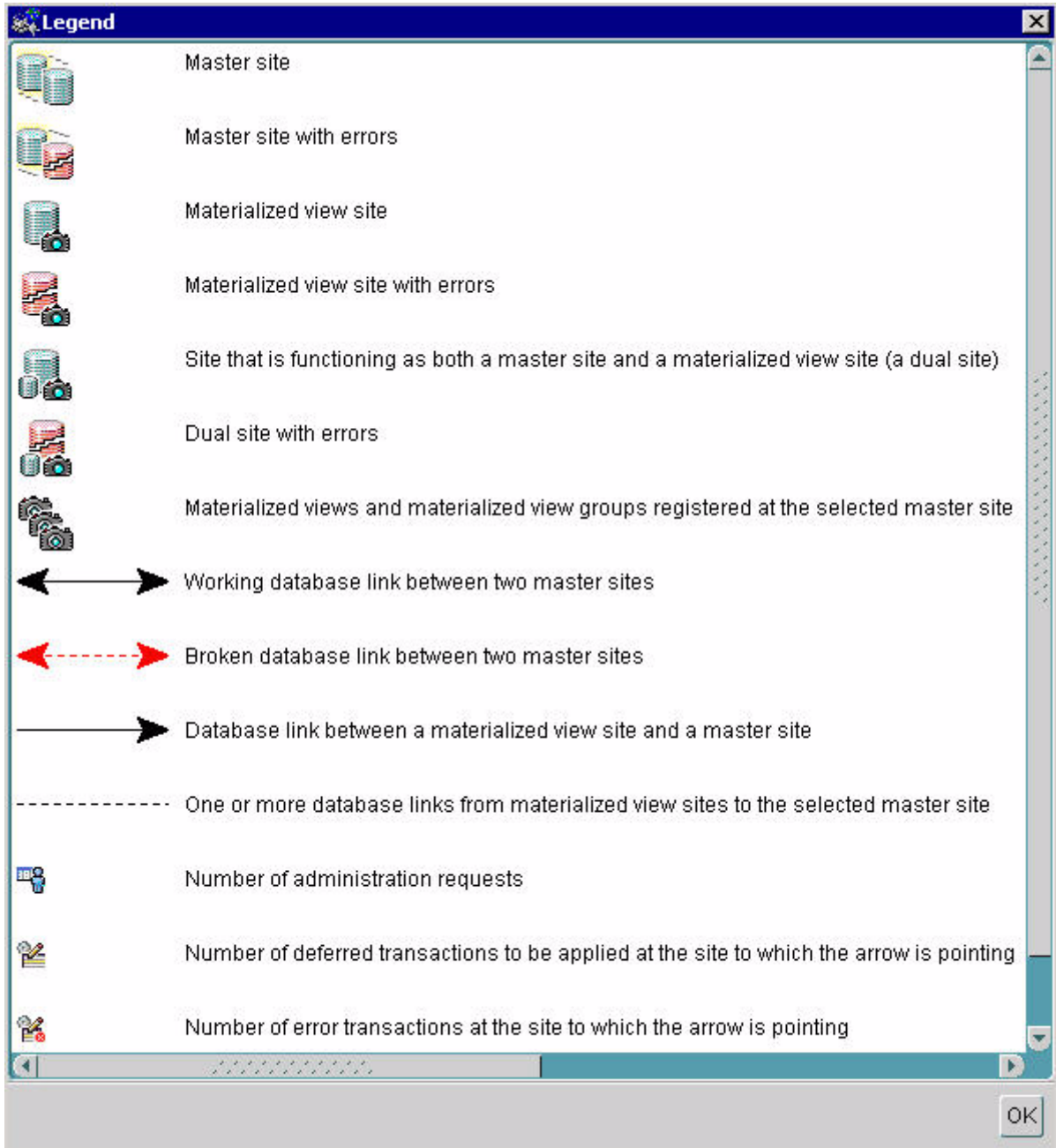
The OEM Console **Administration > Topology** pane opens, displaying the two databases set up in replication mode.



The black arrow between the two database icons indicates that everything is normal. When replication is broken, the arrow turns red.

- 4 Click **Legend** to display a listing of the database state topology icons and what they mean.

The **Legend** window opens.



- 5 If a replication job is broken, then the operator must correct and reschedule the job as follows:
 - a To correct and reschedule a replication job, select the **DBMS Jobs** tab.
 - b Select the required job and click **Edit**.
The **Edit Job** window opens.

Edit Job

Job Number: 1

Status: Normal

Failures: 0

User: REPADMIN

Scheduling

Next Date: 19-Nov-2002 11:13:02 AM Set...

Interval: sysdate+30/86400 Set...

Last Date: 19-Nov-2002 11:12:31 AM

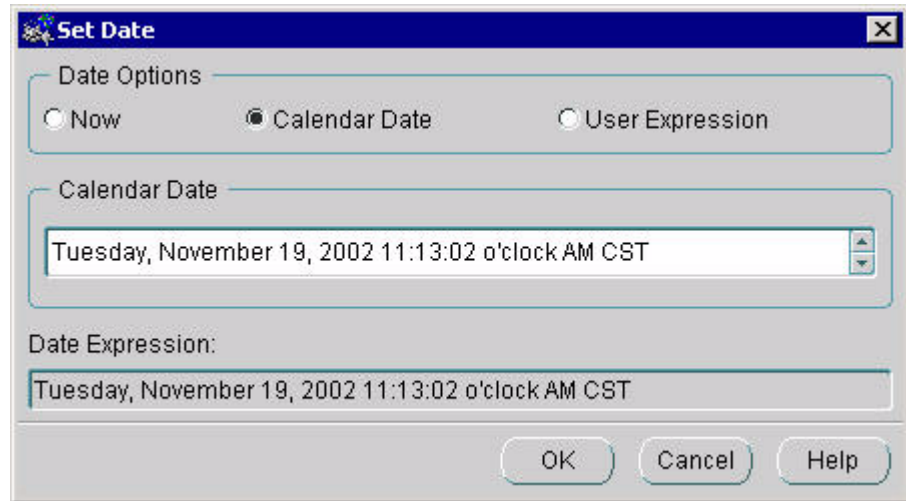
Job Definition:

```
declare rc binary_integer; begin rc := sys.dbms_defer_sys.push (destination=>'MSDB1.PRIMARY', parallelism=>4); end;
```

OK Cancel Help

- c In the **Edit Job** window, change the job status to **Normal**.

- d Beside the **Next Date** field, click **Set**.
The **Set Date** window opens.



- e Select a **Now** and click **OK**.
The job is now rescheduled to run every 30 seconds.

Monitoring registration deletions

Apart from replication jobs, one other job runs periodically to delete expired registrations from the database. This job runs daily and the default setting is every night at 3:00 AM.

The following procedure shows how to monitor the registration deletion job.

On the OEM console

- 1 Login to the primary database as **imsdba**.
- 2 Expand the tree to view **Distributed > Advanced Replication > Administration**.
- 3 Select the **DBMS Jobs** tab.

The nightly registration deletion job displays here.

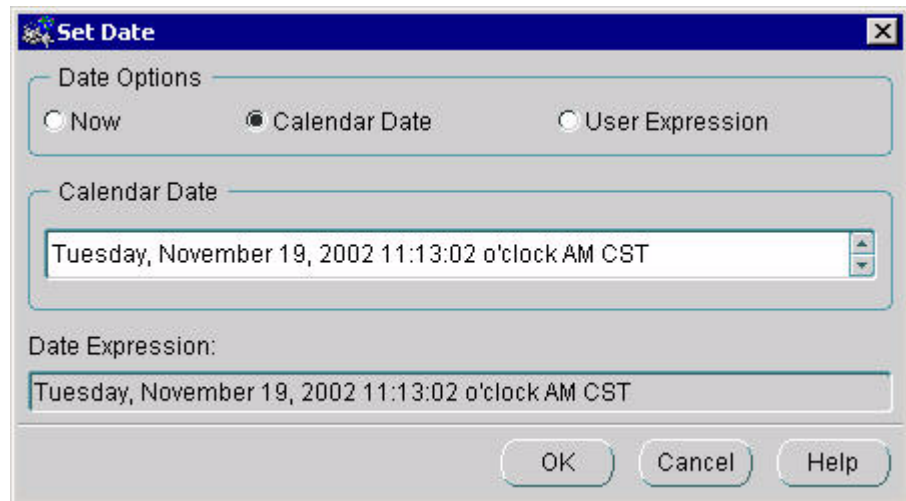
- 4 If the job is broken for any reason, you can correct it as follows:
 - a Select the job and click **Edit**.
The **Edit Job** window opens.

The screenshot shows the 'Edit Job' dialog box with the following details:

- Job Number: 1
- Status: Normal
- # Failures: 0
- User: IMSDBA
- Scheduling section:
 - Next Date: 12-Jan-2003 03:00:00 AM
 - Interval: TRUNC(SYSDATE)+1+3/24
 - Last Date: 11-Jan-2003 03:00:01 AM
- Job Definition: ClearExpiryRegUser;
- Buttons: OK, Cancel, Help

- b In the **Edit Job** window, change the job status to **Normal**.

- c Beside the **Next Date** field, click **Set**.
The **Set Date** window opens.



- d Select **Now** and click **OK**.

Alarm monitoring

Database alarms display from the System Management Console.

For details about using the **Alarm Browser**, see *MCP System Management Console Basics*.

Monitoring alarms

Alarms provide information about Critical, Major, or Minor events affecting the Database Module and other applications. Alarms are used to troubleshoot problems.

From the System Management Console

- 1 Expand the **System** tree and select the **Components** folder.
- 2 On the **Tools** menu, select **Alarm Browser**.
The **Alarm Browser** window displays any current alarm logs.
- 3 In the **Alarm Browser**, double-click the alarm entry to display **Alarm Details**.

The screenshot shows the 'Alarm Browser' window with the following table of alarms:

TimeStamp	Severity	Originator	AlarmName	ProbableCause	FamilyName	AlarmNumber	CLR
Nov 12, 12:56:52	Warning	IMS main database	First Positive Gain...	thresholdCrossed	IMS-OAM	943	
Nov 12, 12:56:52	Minor	IMS main database	Second Positive G...	thresholdCrossed	IMS-OAM	944	
Nov 12, 12:56:52	Minor	IMS main database	Second Positive G...	thresholdCrossed	IMS-OAM	944	
Nov 12, 12:56:52	Major	IMS main database	Maximum Thresho...	thresholdCrossed	IMS-OAM	945	

Below the table, the status bar indicates: Total Alarms: 4 (0 Critical, 1 Major, 2 Minor, 0 Cleared)

The 'Alarm Details' section is currently empty.

At the bottom of the window, there are four buttons: Stop Auto Refresh, Refresh, Clear Details, and Remove Cleared Alarms.

Alert log and trace file monitoring

When a new error message appears in the **alert_imsdb1.log** file, an event is displayed on the OEM Console, as explained in “Monitoring events” on page 24.

Operators can also observe details in alert logs and trace files as explained in the following procedure. See “Fault management” on page 8.

Alert logs and trace files are located in the **bdump** directory as follows:

- **\$ORACLE_BASE/admin/imsdb1/bdump**

ATTENTION

Nortel Networks recommends that you monitor database alert logs and trace files periodically to ensure there are no errors occurring in the Database Module.

Monitoring alert logs and trace files

In a telnet window

- 1 Login as **oracle** to the primary or secondary database where the error message has been reported.
- 2 Navigate to the directory containing the database as follows:
cd \$ORACLE_BASE/admin/imsdb1
If there are errors, the trace files corresponding to these errors are stored in the **bdump** or **udump** directories. Alert logs are stored in the **bdump** directory.
- 3 Open the file in the appropriate directory (for example, **alert_imsdb1.log**) and look for any errors at the end of the file.

Monitoring disk usage

Regularly monitor tablespaces to ensure that they do not run out of disk space. When archive logs are turned on, regular backups are necessary to ensure that the logs are removed and disk space is optimized.

For login instructions, see “OEM Console login” on page 45.

At the Oracle Enterprise Manager

- 1 Login to the OEM Console as **oracle**.
- 2 Select the **Storage** node and expand it.
A list of tablespaces and data files present in the system displays.
- 3 Select each tablespace to determine its size, where it is stored, and how much space is available.

Note: In the unlikely event that a tablespace should become full, contact your next level of support for assistance.

Reports

You can generate reports about configuration, current status, events, and backup jobs from the OEM Console as required. See “Recommended reports” on page 39.

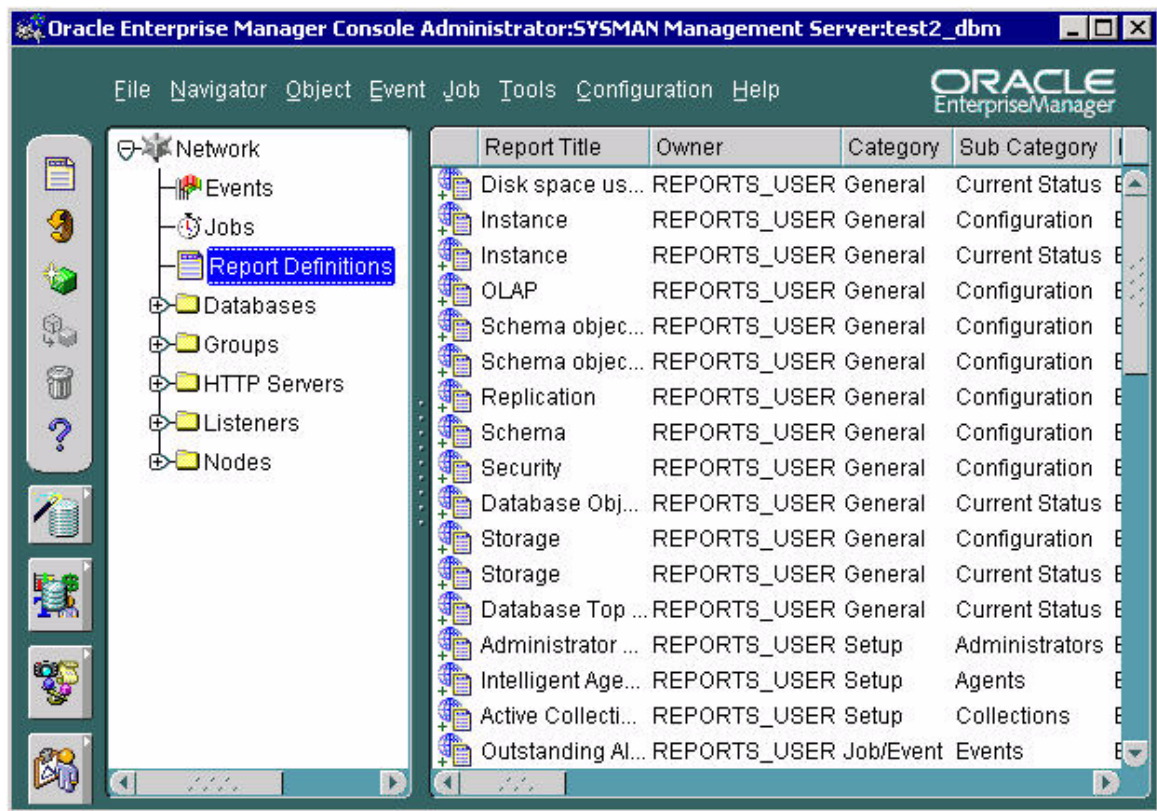
Generating reports

For login instructions, see “OEM Console login” on page 45.

From the OEM Console

- 1 Select the **Report Definitions** menu.

The **Report Definitions** window opens, displaying all available reports.



- 2 Double-click the name of the report you want to view to open it.
The **Edit Report > General** tab opens.

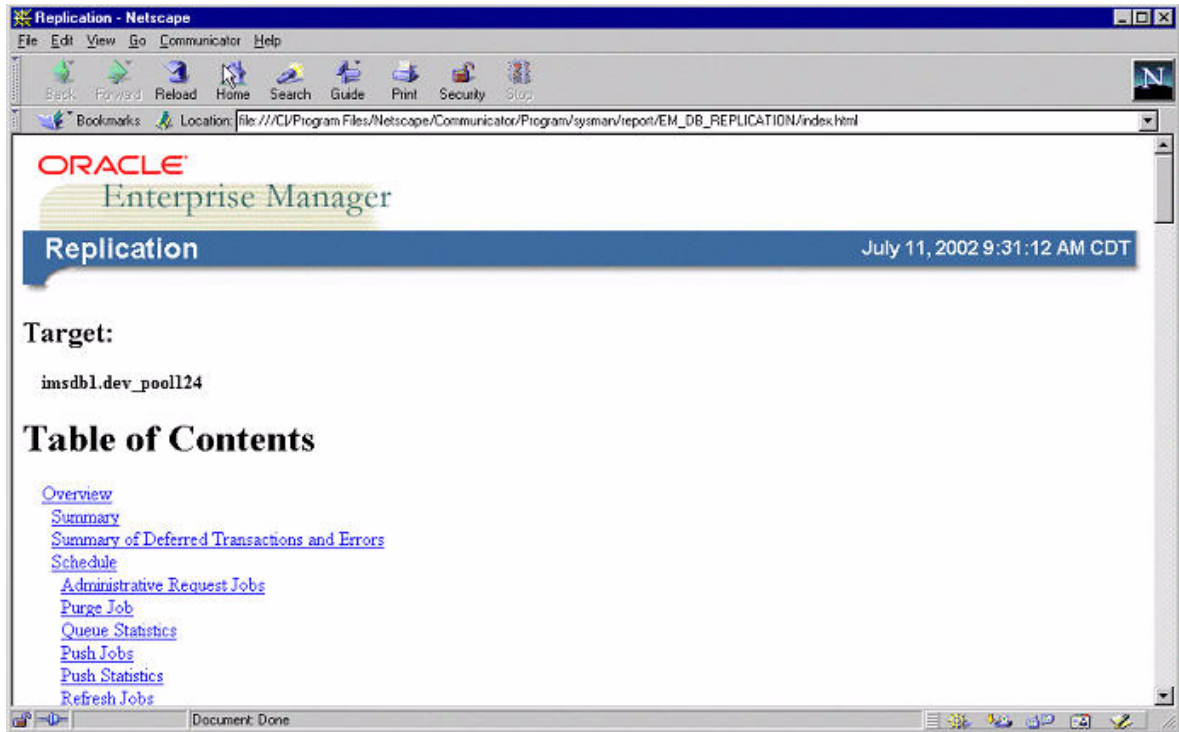
The screenshot shows the 'Edit Report - EM_DB_DiskSpaceForTables' dialog box with the 'General' tab selected. The dialog has four tabs: 'General', 'Elements', 'Parameters', and 'Publish'. The 'General' tab contains the following fields and options:

- Definition Name: EM_DB_DiskSpaceForTables
- Owner: REPORTS_USER
- Report Title: Disk space used by tables
- Report Description: Shows disk space used by tables
- Category: General
- Subcategory: Current Status
- Publish to Enterprise Manager reporting website
- Report Type: Database
- Create individual reports for all targets of selected type
- Create a single report for the targets selected below
- Selected Targets: (Empty list)
- Available Targets: backupdb.test2_dbm, imsd1.test2_dbm
- Buttons: Add, Remove
- Bottom buttons: View Report..., Save As..., OK, Cancel, Help

- 3 Select **Create a Single Report for the Targets Selected Below**.
- 4 Select the appropriate database from the **Available Targets** list and click **Add** to add it to the **Selected Target** list.

5 Click View Report.

The chosen report is displayed in the default web browser.



Recommended reports

It is recommended that the operator generate the following reports regularly.

Table 5 Performance management task flows

Report Title	Category	Description
Replication	Configuration	Shows detailed configuration and statistics of a replicated system
Storage – Configuration	Configuration	Displays status and size of all storage objects
Database Object Space Usage	Current Status	Shows space usage reports for database objects

Table 5 Performance management task flows

Report Title	Category	Description
Disk space used by tables	Current Status	Shows disk space used by tables
Instance	Current Status	Displays instance statistics and process state
Outstanding Alerts Sorted by Target	Events	Displays details, sorted by target name, on all outstanding alerts with status of critical, warning, unknown or error
Failed Jobs from Last 7 Days	Jobs	Lists all jobs that failed in the last 7 days
Average Execution Time per Job	Jobs	Shows information on execution times for jobs completed against a target
Registered Events Sorted by Target	Event	Provides information, sorted by target, for all registered events

The Oracle Monitor component

On the System Management Console, the Oracle Monitor component provides reporting information about the following areas:

- the **IMS main database** (see “IMS Main and Backup Database tabs” on page 60)
- the **IMS backup database** (see “IMS Main and Backup Database tabs” on page 60). By default, the Oracle Monitor for this database is deactivated. The Oracle Monitor for the IMS backup database should only be activated if scheduling **RMAN** backups.
- the **Oracle Server** (see “Oracle Server tab” on page 62)
- **Oracle Listeners** (see “Oracle Listener tab” on page 63)

Depending on the information collected, a log, alarm or OM can be generated.

ATTENTION

The Oracle Monitor component does not monitor the Database Module in real time. For details about viewing and responding to alarms in real time, see “Alarm monitoring” on page 34.

Information regarding the Oracle Monitor component appears in the **Oracle Monitor General Information Area (GIA)** pane when the root level of the Oracle Monitor component is selected within the System Management Console. See Figure 4, “Oracle Monitor: General Information Area (GIA) pane”.

Note: The name of the Oracle Monitor component is customer configurable and may appear differently in your configuration.

Figure 4 Oracle Monitor: General Information Area (GIA) pane

PriOra Details

General		States	
Component Type:	Oracle Monitor (Small)	Administrative:	UNLOCKED
OS Type:	all	Operational:	ENABLED
Version:	ims_1.1_build268		
Services:	12		
DB Info		Alarms	
Database Mode:	Replicated	Critical:	0
Number of Replication Conflicts:	0	Major:	0
Replication Queue Size:	0	Minor:	0
Number of Broken Jobs:	0		

States			Alarms		
Service	Administrative	Operational			
IMS backup database	UNLOCKED	ENABLED			
Database Base	UNLOCKED	ENABLED			
DetailedLogCollector	UNLOCKED	ENABLED			
IMS main database	UNLOCKED	ENABLED			
Oracle Listeners	UNLOCKED	ENABLED			
Oracle Server	UNLOCKED	ENABLED			
OssLSCFacade	UNLOCKED	ENABLED			
OssMgmtAgent	UNLOCKED	ENABLED			
OssTCFME	UNLOCKED	ENABLED			
Trap Dispatcher	UNLOCKED	ENABLED			
TssAgent	UNLOCKED	ENABLED			
TssLogManager	UNLOCKED	ENABLED			

The **Alarms** tab shown in Figure 5, "Oracle Monitor: GIA Alarms tab pane" lists the number of Critical, Major, and Minor alarms.

Figure 5 Oracle Monitor: GIA Alarms tab pane

States		Alarms		
Service	Critical	Major	Minor	
IMS backup database	0	0	0	
Database Base	0	0	0	
DetailedLogCollector	0	0	0	
IMS main database	0	0	0	
Oracle Listeners	0	0	0	
Oracle Server	0	0	0	
OssLSCFacade	0	0	0	
OssMgmtAgent	0	0	0	
OssTCFME	0	0	0	
Trap Dispatcher	0	0	0	
TssAgent	0	0	0	
TssLogManager	0	0	0	



Configuration management

Strategy

Nortel Networks performs initial configuration of the Oracle Replication Server and Oracle Enterprise Manager during installation. The **sysman** and **oracle** accounts are also part of initial installation.

This chapter documents configuration tasks that can be performed after initial installation.

Tasks

Table 6 lists Database Module configuration tasks.

Table 6 Configuration management tasks

Topic	Subtopic	Procedure
Login	Oracle Enterprise Manager Console	“Logging in to the OEM Console” on page 45
Configuration	Email notifications	“Configuring the sysman user in OEM to receive email notifications” on page 49
	Read-only user	“Configuring a database observer account from the OEM Console” on page 56
System Management Console		“Application database connection configuration” on page 57

Tools and utilities

Use the following tools for Database Module configuration:

- System Management Console: Launches the OEM Console and Oracle Monitoring Application. Provides log and alarm information. For details, see MCP System Management Console Basics.
- Oracle Enterprise Manager (OEM) Console: Used by the database administrator for backup and recovery and database fault management.

For details, see “Security and Administration” on page 69 and “Fault management” on page 17.

OEM Console login

This section explains how to login to the OEM Console from the System Management Console.

ATTENTION

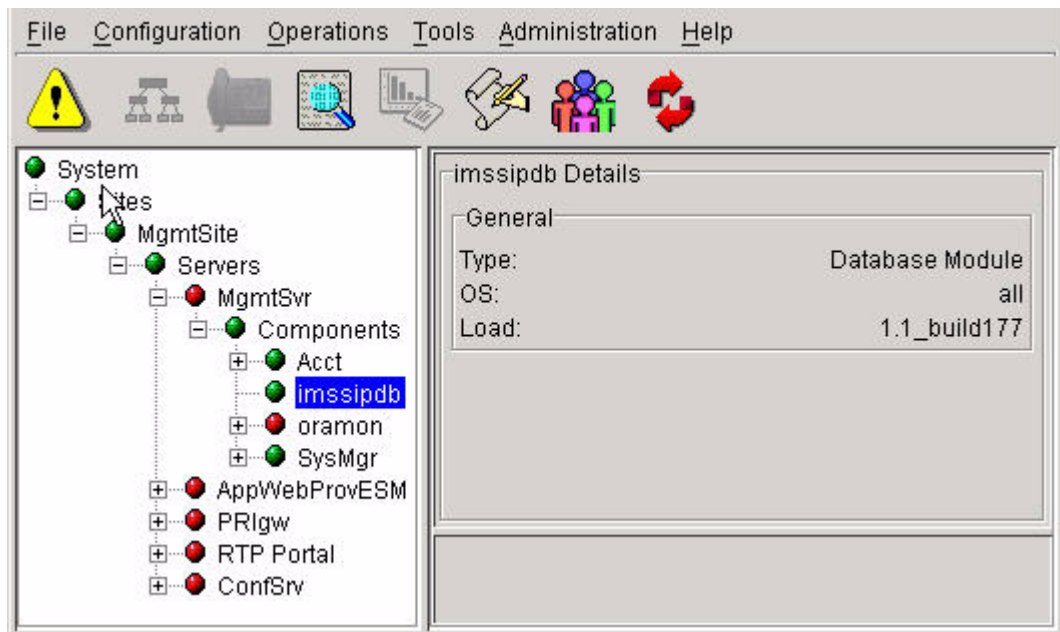
Only database administrators and system administrators have access to the Database Administration option in the System Management Console window.

Logging in to the OEM Console

Login to the OEM Console from the System Management Console or from a web browser on a server within the network.

From the System Management Console

- 1 Navigate to the Database Module as shown in the following figure:



- 2 Right-click the **imssipdb** database folder and select **Database Administration**.

The **Confirm IP Address** dialog box opens.

- 3 Enter the **imssipdb** database IP address provided during installation.

The **Launch the Oracle Enterprise Manager Console** web page opens.

- a Bookmark the OEM Console URL for future use from any system within the network.



ORACLE
Enterprise Manager

Launch the Oracle Enterprise Manager Console

The Enterprise Manager Console allows you to centrally manage and administer your environment. To launch the Console, enter the machine name on which your Oracle Management Server runs and then click the button labeled "Launch Console".

Oracle Management Server:

Access Oracle Enterprise Manager Reports

Enterprise Manager reports allow users to quickly view and analyze information about their managed systems. To view reports that have been published to the web, enter the machine name on which your Enterprise Manager reporting web server runs and the port on which it listens and then click the button labeled "Access Reports".

Reporting Web Server: Port:

Copyright © 2000, Oracle Corporation. All Rights Reserved.

Information

- [Documentation](#)
- [Release Notes](#)
- [Quick Tours](#)

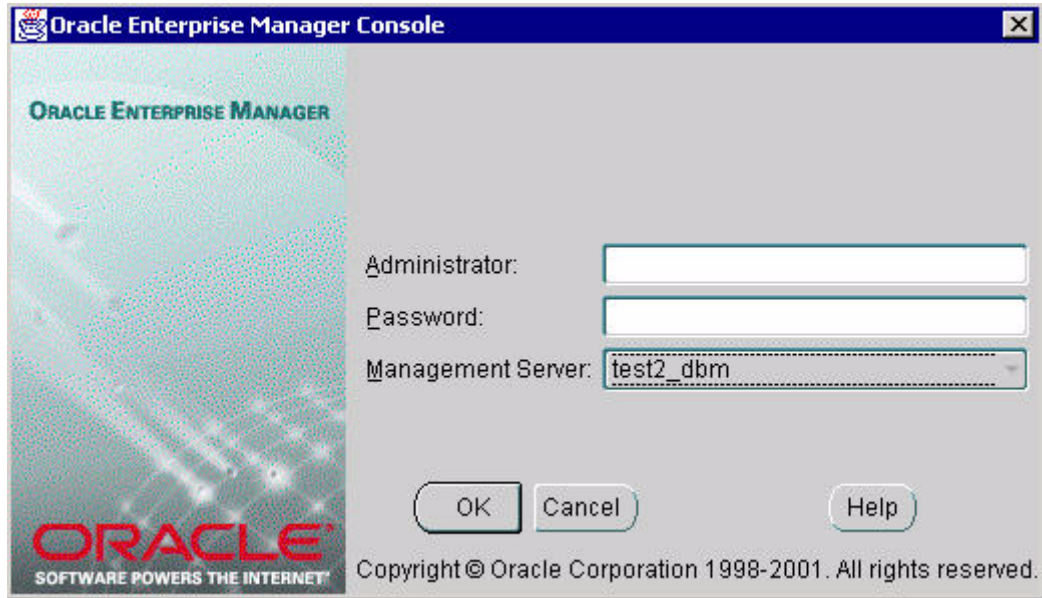
Useful Links

- [Oracle Home Page](#)
- [Enterprise Manager Home Page](#)
- [Support Home Page](#)
- [Download Plug-in](#)
- [Accessibility Setup](#)

- 4 In the **Oracle Management Server** box shown in step 3, enter the node name of the server containing the primary database and click **Launch Console**.

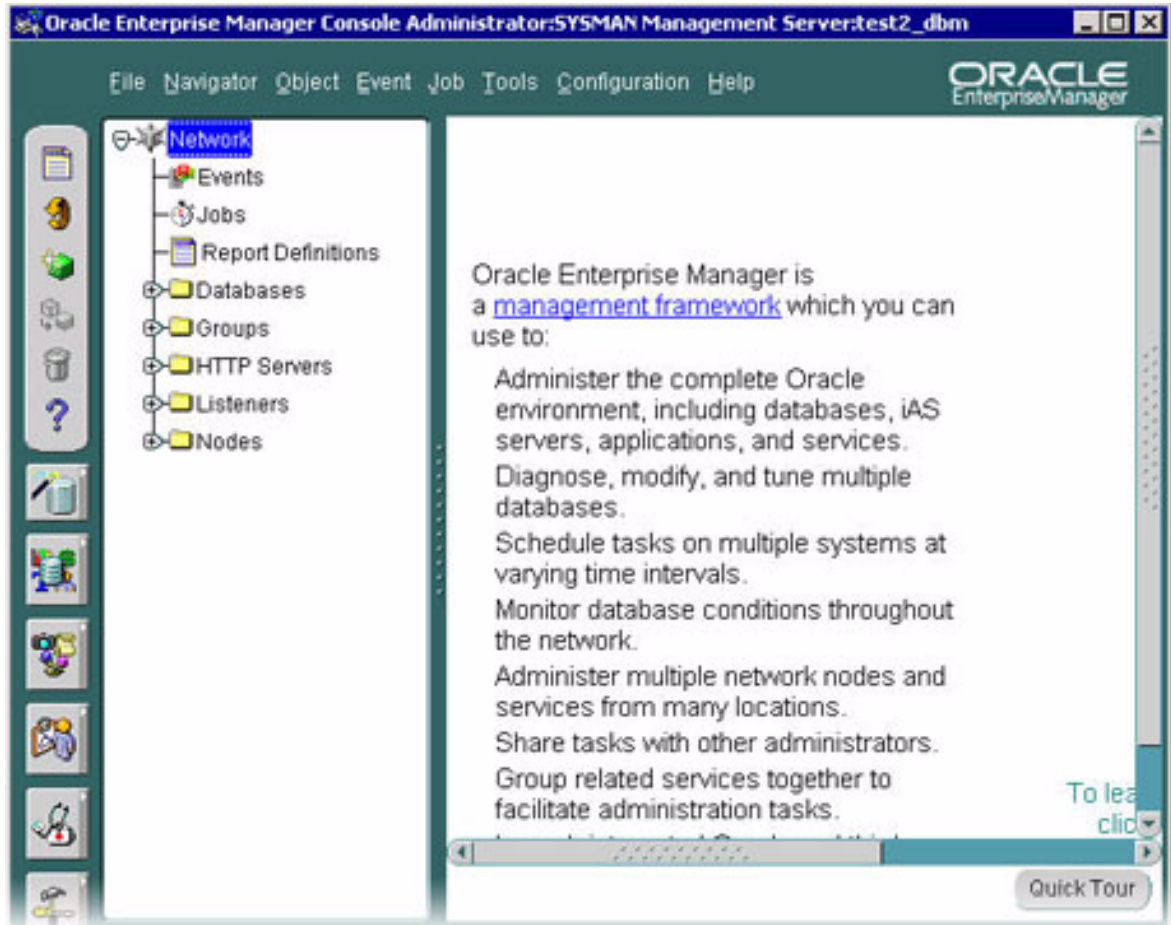
The **Oracle Enterprise Manager Console** login window opens.

Figure 6 Oracle Enterprise Manager Console login window



- 5 Enter the **sysman** user name and password provided during installation and click **OK**. The **Oracle Enterprise Manager Console** opens as shown in Figure 7.

Figure 7 Oracle Enterprise Manager Console



Configuration tasks

This section includes the following procedures:

- “Configuring the sysman user in OEM to receive email notifications” on page 49
- “Configuring a database observer account from the OEM Console” on page 56

Configuring the sysman user in OEM to receive email notifications

Use the following procedure to configure the **sysman** user in OEM to receive email notifications about backup results.

Administrative rights are configured and user names, passwords, server names and IP addresses are provided during installation.

From the System Management Console

- 1** Launch the **Oracle Enterprise Manager** web page.
The **Oracle Enterprise Manager Console** login window opens. See Figure 6, “Oracle Enterprise Manager Console login window,” on page 47.
- 2** Login as **sysman**.
The **Oracle Enterprise Manager Console** opens. See Figure 7, “Oracle Enterprise Manager Console,” on page 48.

- 3 From the **OEM Configuration** menu, select **Configure Paging and Email**.

The **Configure Paging/Email** dialog box opens.



- 4 Type in the **SMTP Mail Gateway** and **Sender's SMTP Mail Address** (provided during installation) and click **OK**.
- 5 From the **Configuration** menu, select **Manage Administrators**.

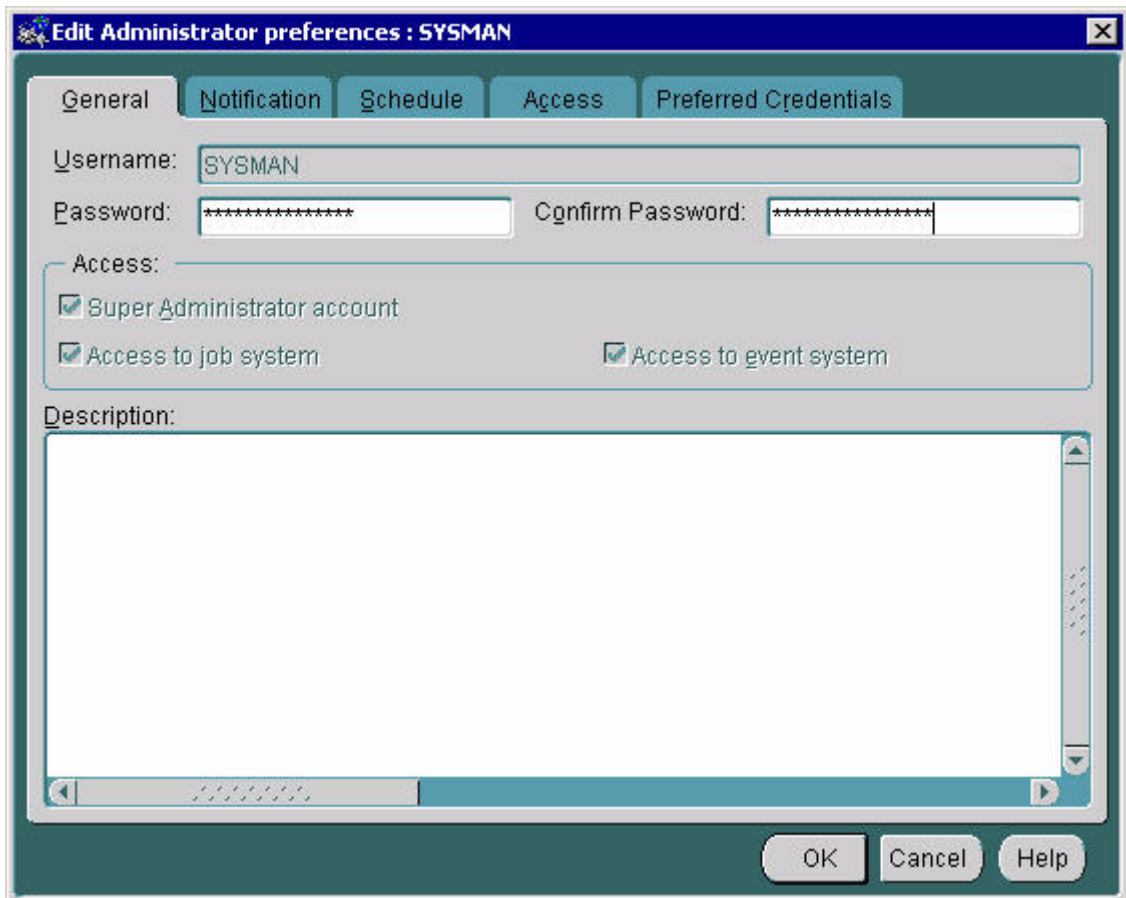
The **Manage Administrator Accounts** window opens as shown in Figure 8.

Figure 8 Manage Administrator Accounts window

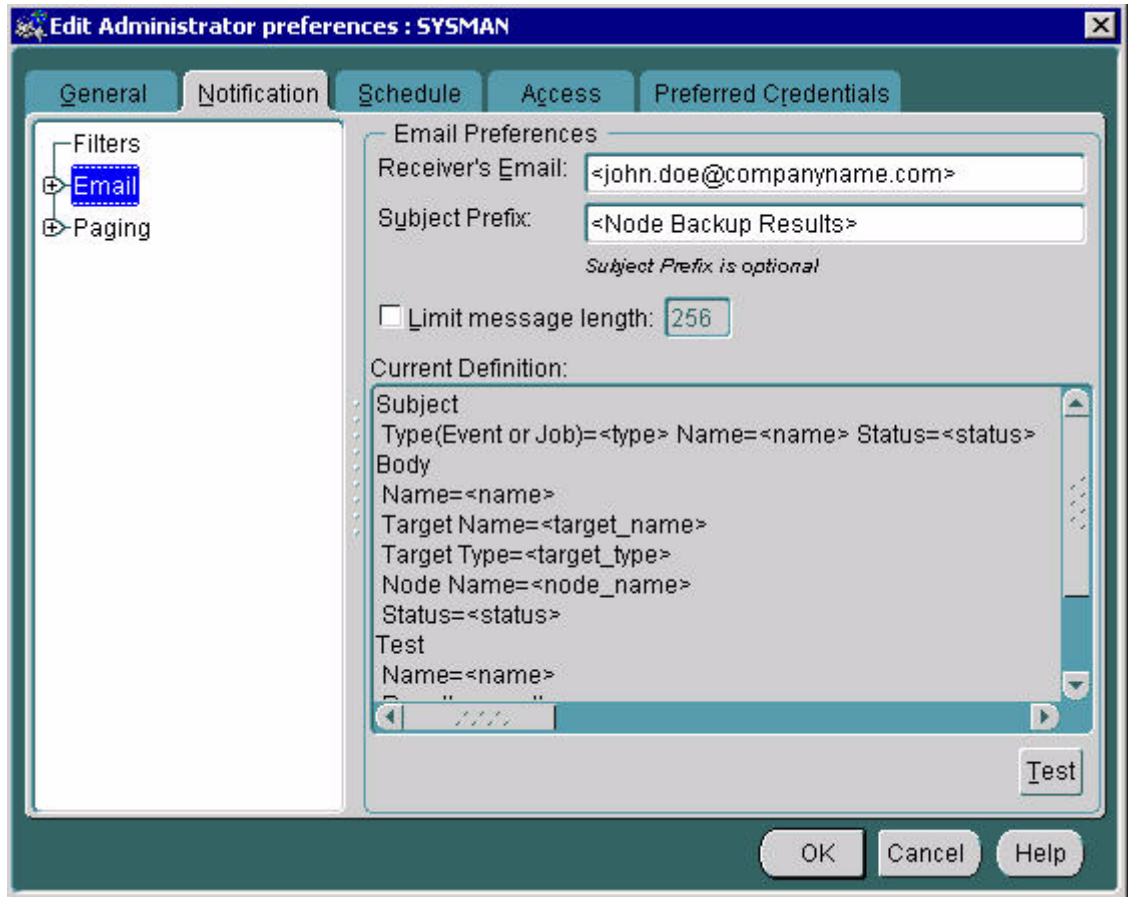


- 6 Select **SYSMAN** and click **Edit**.

The **Edit Administrator Preferences > General** window opens.



- 7 Select the **Notification** tab and click **Email**.
- 8 Type in the **Receiver's Email** and **Subject Prefix**, then click **Test**.

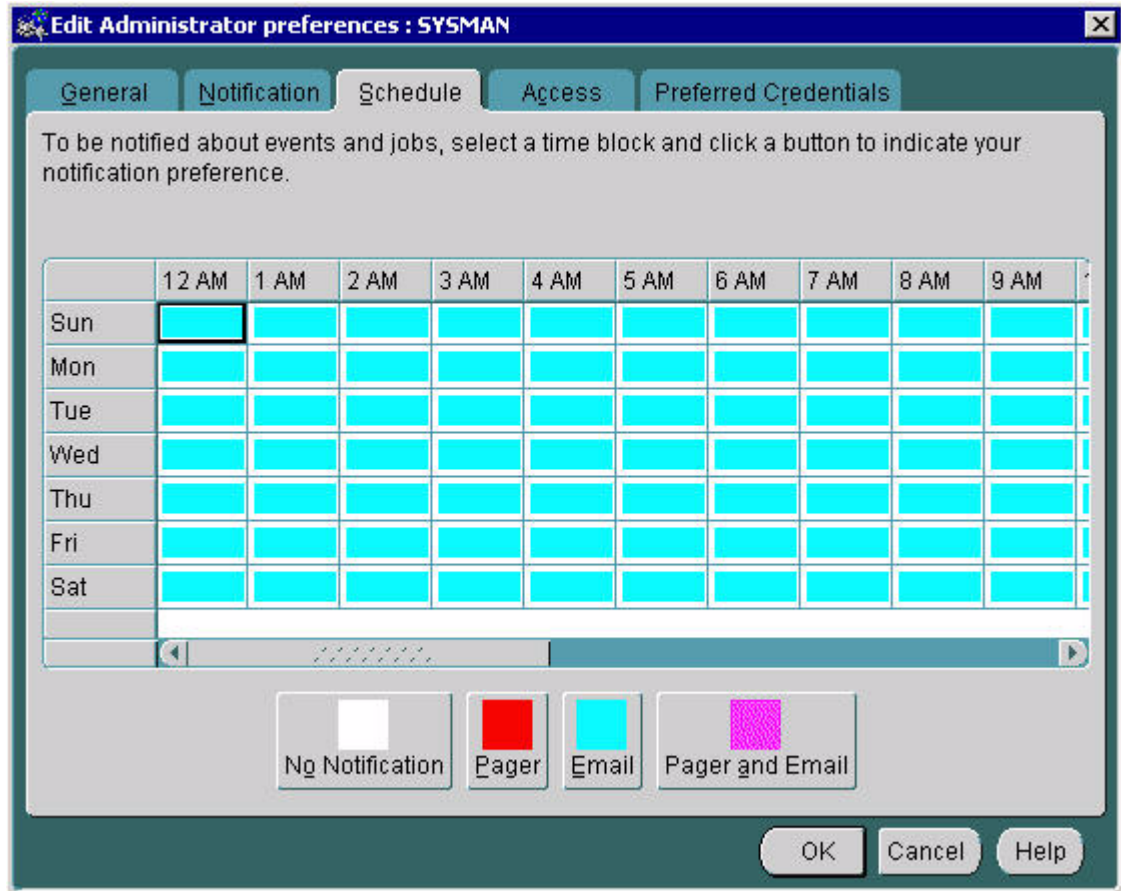


This step sends a test email to the receiver.

- 9 Do either of the following:
 - If the email arrives at the specified address, proceed to the next step.
 - If the email is not sent and an error message results, check with your administrator to obtain a valid **Receiver's Email**.

10 Select the **Schedule** tab.

The **Edit Administrator Preferences > Schedule** tab opens.

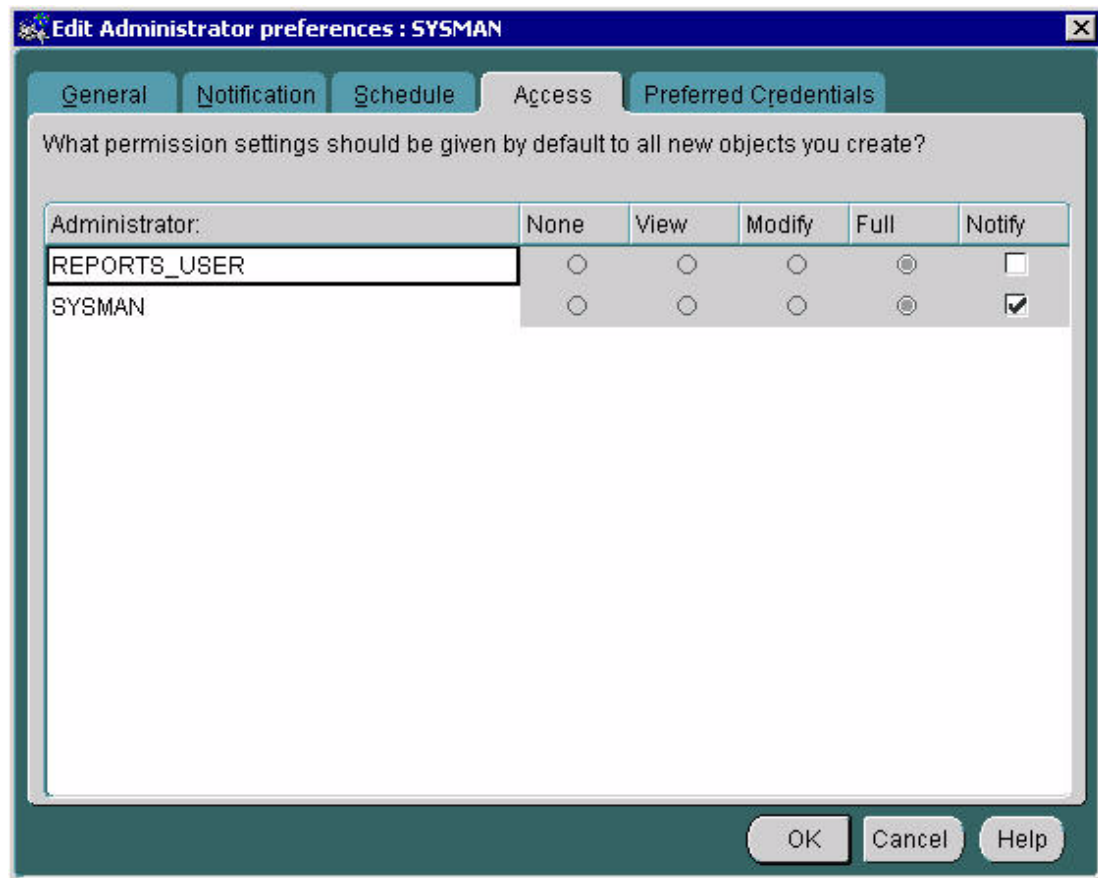


11 Click the **Email** icon and select all days of the week and all hours of the day as follows:

Click the top left-hand cell of the grid and drag the mouse pointer to the bottom right-hand cell.

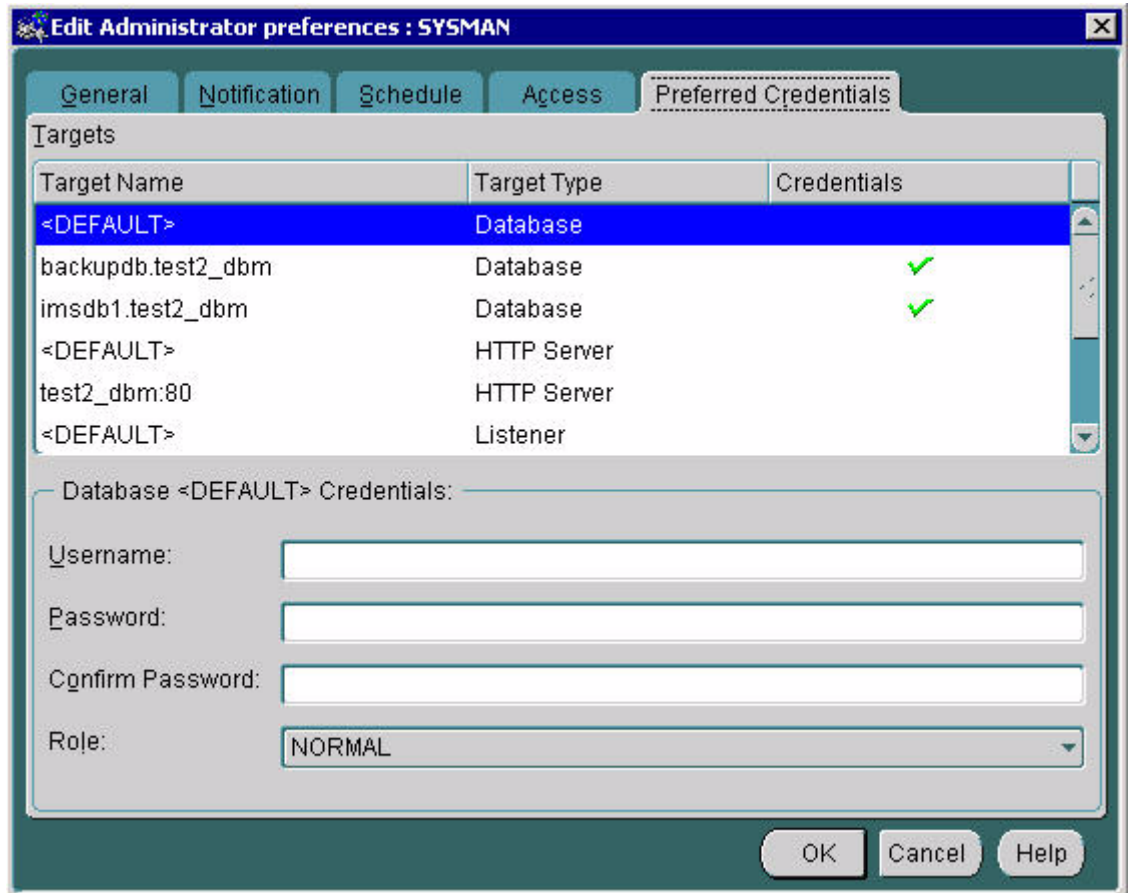
12 Select the **Access** tab.

The **Edit Administrator Preferences > Access** tab opens.



- 13 Select the **Notify** option for the **sysman** user and click the **Preferred Credentials** tab.

The **Edit Administrator Preferences > Preferred Credentials** tab opens.



- 14 Under **Targets**, select the **<DEFAULT> Target Name** with the Node **Target Type**.
- 15 Enter the correct **Username** and **Password** for the **oracle** user and click **OK** to save all changes and close the **Edit Administrator Preferences** dialog box.

Configuring a database observer account from the OEM Console

The following procedure explains how to set up observer accounts from the OEM Console for the Database Module. Observer accounts are used to monitor the databases.

From the System Management Console

- 1** Launch the **Oracle Enterprise Manager** web page.
The **Oracle Enterprise Manager Console** login window opens. See Figure 6 on page 47
- 2** Login as **sysman** using the password supplied during installation.
The **Oracle Enterprise Manager Console** opens. See Figure 7, "Oracle Enterprise Manager Console," on page 48.
- 3** From the **Configuration** menu, select **Manage Administrators**.
The **Manage Administrator Accounts** window opens. See Figure 8 on page 51.

- 4 Select **SYSMAN** and click **Add**.

The **Create Administrator Account** window opens.



- 5 Enter a **Username** and **Password** for the observer account and click **OK**.

Application database connection configuration

The following applications have a service called Database, DB_Factory, or Database Base where the console operator must configure database IP addresses as part of their configuration.

- Oracle Monitor
- IP Client Manager
- SIP Application Module
- Management Module
- Provisioning Module
- SIP Web Client Manager
- SIP Audio Server (connects only during initialization)

For details about configuring application connections to the Database Module, see the related component documents. Table 7 lists the configuration properties used by applications to set up access to the Database Module.

Table 7 Application database configuration properties

Property name	Format	Description
Primary Host	Type: String Range: Not applicable Default IP address: 0.0.0.0	Designates the IP address of the primary database
Secondary Host	Type: String Range: Not applicable Default IP address: 0.0.0.0	Designates the IP address of the secondary database
Connections	Type: Integer Range: Not applicable Default: 1-16	Displays the maximum number of connections the selected application has to the database Note: Do not change the Connections value. The number of connections required varies between applications.

Querying or modifying Oracle Monitor configuration properties

The System Management Console displays administrative and operational states, as well as snapshot alarm information. Administrative state information reflects the condition of the application being monitored. For details about alarm monitoring, see “Alarm monitoring” on page 34.

From the System Management Console

- 1 Open the **Components** folder, and select the root level **Oracle Monitor** component.

Information displays in the **GIA** pane. See Figure 4, “Oracle Monitor: General Information Area (GIA) pane,” on page 42.

- 2 To query the configuration properties of a **Oracle Monitor** component, right-click the root level **Oracle Monitor** component for the primary database or secondary database you want to query and click **Query**.

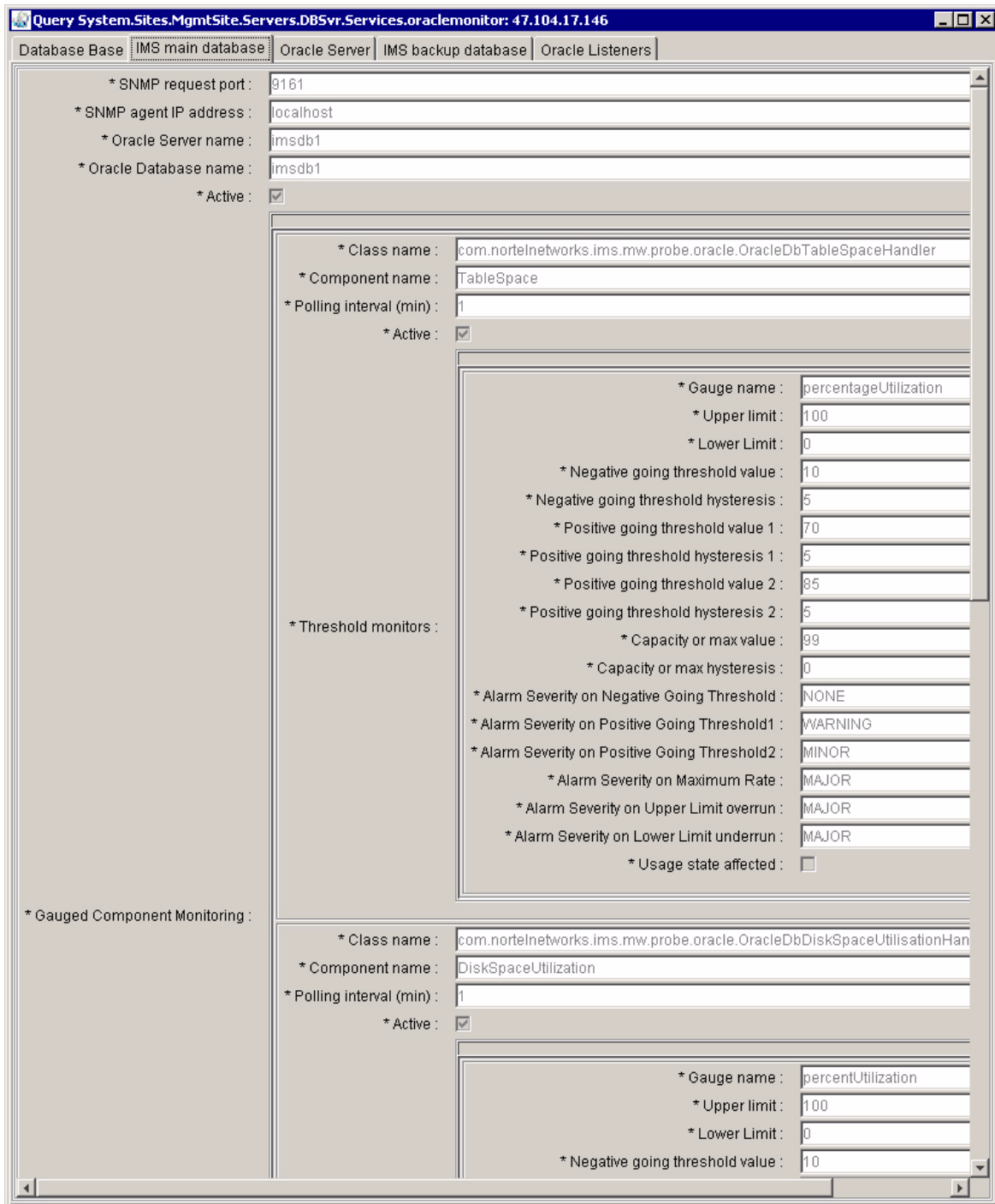
The **Query Oracle Monitor** dialog box displays the properties.

- 3 To modify the configuration properties of a **Oracle Monitor** component, do the following:
 - a Right-click the root level **Oracle Monitor** component and click **Lock** to lock the component while you modify the settings.
 - b A confirmation dialog box prompts you to confirm that you want to lock the **Oracle Monitor**. Click **Yes**.

Note: Locking the **Oracle Monitor** has no effect on the component being monitored (in this case the primary or secondary database).
 - c Right-click the root level **Oracle Monitor** component and click **Modify**.
 - d Modify the properties as required and click **OK**.

IMS Main and Backup Database tabs

The following figures show the fields available for query or modification from the **IMS Main Database** and **IMS Backup Database** tabs of the **Query** or **Modify Oracle Monitor** dialog box:



Query System.Sites.MgmtSite.Servers.DB5vr.Services.oraclemonitor: 47.104.17.146

Database Base | **IMS main database** | Oracle Server | IMS backup database | Oracle Listeners

* Threshold monitors :

- * Positive going threshold value 2 : 85
- * Positive going threshold hysteresis 2 : 5
- * Capacity or max value : 99
- * Capacity or max hysteresis : 0
- * Alarm Severity on Negative Going Threshold : NONE
- * Alarm Severity on Positive Going Threshold1 : WARNING
- * Alarm Severity on Positive Going Threshold2 : MINOR
- * Alarm Severity on Maximum Rate : MAJOR
- * Alarm Severity on Upper Limit overrun : MAJOR
- * Alarm Severity on Lower Limit underrun : MAJOR
- * Usage state affected :

* Component Monitoring :

- * Handler class name : com.nortelnetworks.ims.mw.probe.oracle.OracleDbBlockGetRateHandler
* Component name : BlockGetRate
* Polling interval (min) : 1
* Active :
- * Handler class name : com.nortelnetworks.ims.mw.probe.oracle.OracleDbOpStatusHandler
* Component name : OperationalStatus
* Polling interval (min) : 1
* Active :
- * Handler class name : com.nortelnetworks.ims.mw.probe.oracle.OracleDbDataFileHandler
* Component name : DataFile
* Polling interval (min) : 1
* Active :
- * Handler class name : com.nortelnetworks.ims.mw.probe.oracle.OracleDbCacheHitRatioHandler
* Component name : CacheHitRatio
* Polling interval (min) : 1
* Active :

* Trap handlers :

- * Trap handler class name : com.nortelnetworks.ims.mw.probe.oracle.OracleDatabaseTrapHandler
* Trap handler name : oracleDBTrapHandler
* Active :

Database Base tab

The following figure shows the fields available for query or modification from the **Database Base** tab of the **Query** or **Modify Oracle Monitor** dialog box:

The screenshot shows a window titled "Query System.Sites.MgmtSite.Servers.DB5vr.Services.oraclemonitor: 47.104.17.146". The "Database Base" tab is selected. The fields are as follows:

* Primary Host :	47.104.17.140
* Connections :	1
Secondary Host :	

Oracle Server tab

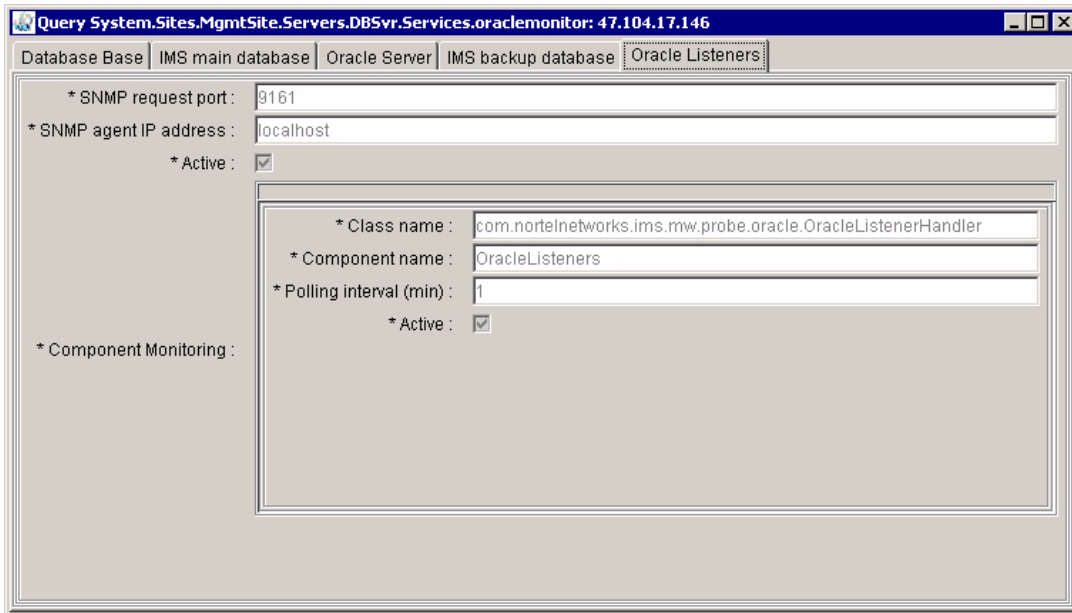
The following figure shows the fields available for query or modification from the **Oracle Server** tab of the **Query** or **Modify Oracle Monitor** dialog box:

The screenshot shows the same window with the "Oracle Server" tab selected. The fields are as follows:

* SNMP request port :	9161
* SNMP agent IP address :	localhost
* Oracle Server name :	imsdb1
* Active :	<input checked="" type="checkbox"/>
* Monitor functions :	
* Handler class name :	com.nortelnetworks.ims.mw.probe.oracle.OracleServerInfoHandler
* Handler name :	GeneralInfo
* Polling interval (min) :	1
* Active :	<input checked="" type="checkbox"/>
* Handler class name :	com.nortelnetworks.ims.mw.probe.oracle.OracleServerOpStatusHandler
* Handler name :	OperationalStatus
* Polling interval (min) :	1
* Active :	<input checked="" type="checkbox"/>

Oracle Listener tab

The following figure shows the fields available for query or modification from the **Oracle Listener** tab of the **Query** or **Modify Oracle Monitor** dialog box:





Accounting management

Strategy

Some information stored in the database is propagated to the Accounting Module. For details, see *MCP Accounting Module Basics*.



Performance management

Strategy

Database logs, alarms, and operational measurements are displayed in the System Management Console. For details, see *MCP System Management Console Basics*.



Security and Administration

How this chapter is organized

This chapter is organized as follows:

- “Security” on page 69
- “Administration” on page 70

The security and administration procedures are performed primarily through the System Management Console. For more information, refer to the *MCP Management Module Basics* and the *MCP System Management Console Basics*.

Security

The Database Module uses Oracle database technology to ensure confidentiality, integrity, and availability of data. All configuration and subscription data held in the Database Module are also protected by user authentication and network firewalls configured in a network architecture.

Basic administrative roles and corresponding privileges are assigned, and user roles and passwords are provided during installation.

Table 8 describes Database Module user accounts.

Table 8 Database Module administrator and user roles

User	Description
oracle	Runs command line scripts and telnet sessions
sysman	Manages administration on the Oracle Enterprise Manager console
root	Superuser account on Sun servers

For Database Module login and user configuration procedures, see “Configuration management”.

For more information about network and Database Module security, see *MCP Basics*.

Administration

Database Module administration consists of backup, recovery, resynchronization, and optimization.

Replication objects are grouped together to form a replication group. Administration of the Database Module replication process is performed through a replication group called IMSREPGROUP.

Tasks

Table 9 outlines Database Module Administration tasks.

Table 9 Administration tasks

Topic	Subtopic	Procedure
"Database backups"	Parameter files	"Backing up parameter files" on page 73
	"Oracle Enterprise Manager backups"	"Backup job setup" on page 74
	New backup jobs	"Creating a backup job" on page 75
	Existing backup jobs	"Modifying a scheduled backup job" on page 82
"Database recovery"	Export	"Restoring exported backup files" on page 85
	RMAN	"Restoring RMAN backup files" on page 86
	Control files	"Restoring control files" on page 88
Replication	Errors	"Resolving replication errors" on page 89

Table 9 Administration tasks

Topic	Subtopic	Procedure
Resynchronization		“Resynchronizing databases” on page 93
Disk space management	Database disk usage	“Optimizing database disk usage” on page 94

Tools and utilities

The Database Module uses the following administrative tools:

- Oracle Enterprise Manager (OEM) Console: Used by the database administrator for backup and recovery and database fault management.

For details, see “Fault management” on page 17.

- Recovery Manager (RMAN), an Oracle tool used to automate backup and restore with archive logs turned on.

Database backups

In addition to the redundancy provided by Oracle replication, the OEM Console supports scheduling automated backups of the Database Module as often as required.

The following two types of backups are supported in the Database Module:

- Backup and restore using export and import of data

OR

- Backup and restore using Recovery Manager (RMAN)



CAUTION

Using Recovery Manager (RMAN), archive logs can fill up available disk space if backups are not done regularly.

It is recommended that the Export/Import method be used to backup and restore data.

Table 10, “Comparing backup and recovery methods,” on page 72 outlines the major differences between the two types of backups.

Table 10 compares the Export/Import and RMAN backup and recovery methods.

Table 10 Comparing backup and recovery methods

Export/Import method	RMAN method
Simple to perform	More functionality but more complicated to perform
No archive logs	Archive logs could fill up disk space if regular backups are not scheduled
Incremental backups are not available	Incremental backups are available
Point-in-time recovery is not available. During recovery, data written between the last backup and the point of failure is lost	Point-in-time recovery is available. During recovery, data written between the last backup and the point of failure can be recovered
Backups are performed on one database	Backups must be performed on both databases at the same time

Table 10 Comparing backup and recovery methods

Export/Import method	RMAN method
Individual data files cannot be recovered	Individual data files can be recovered
Longer recovery time	Shorter recovery time

Backups should be scheduled during off-peak hours. The default time is 2:00 a.m.

If a backup fails, the log files display the probable cause of the failure and any available explanatory information. To view the log files, double-click a failed job displayed in the OEM Console. See also “Monitoring backups” on page 20.

**CAUTION**

To avoid risk of data loss, always backup data to external media and use consistent and regular backup procedures.

This section contains the following backup procedures:

- “Backing up parameter files” on page 73
- “Backup job setup” on page 74
- “Modifying a scheduled backup job” on page 82

Oracle Enterprise Manager backups

Use the procedures listed in this section to schedule backups. This section explains the generic method for backing up the Database Module using the Oracle Enterprise Manager (OEM).

Similar methods are used to schedule any kind of backup job, the only difference being the script name and the parameters used.

Backing up parameter files

The following procedure is necessary to backup database parameter files on the primary and secondary databases. The (.keep) versions are created in case the original file is corrupted.

Note: Execution of this backup procedure is required only when the version of the Oracle database changes.

At the primary database server command line

- 1 Backup the **initimldb1.ora** file as follows:
cd /opt/app/oracle/admin/imldb1/pfile
cp initimldb1.ora initimldb1.ora.keep
- 2 Backup the **tnsnames.ora** file as follows:
cd /opt/app/oracle/admin/imldb1/pfile
cp tnsnames.ora tnsnames.ora.keep
- 3 Backup the **listener.ora** file as follows:
cd /opt/app/oracle/admin/imldb1/pfile
cp listener.ora listener.ora.keep
- 4 Backup the **sqlnet.ora** file as follows:
cd /opt/app/oracle/admin/imldb1/pfile
cp sqlnet.ora sqlnet.ora.keep
- 5 Repeat this procedure on the secondary database server.

Backup job setup**CAUTION**

Only trained personnel should perform the following task.

Use the following backup procedure to set up daily backup jobs.

Note: This procedure is only needed when scheduling **RMAN** backups.

At the primary database server command line

- 1 Login to the database server as **oracle**.
- 2 Execute the following commands:
cd /IMS/imssipdb/data/db_schema/backup
configure_backup.sh <db_type>
Note: db_type can be PRIMARY or SECONDARY.
- 3 Repeat this procedure on the secondary database server.

For login instructions, see “OEM Console login” on page 45.

Creating a backup job



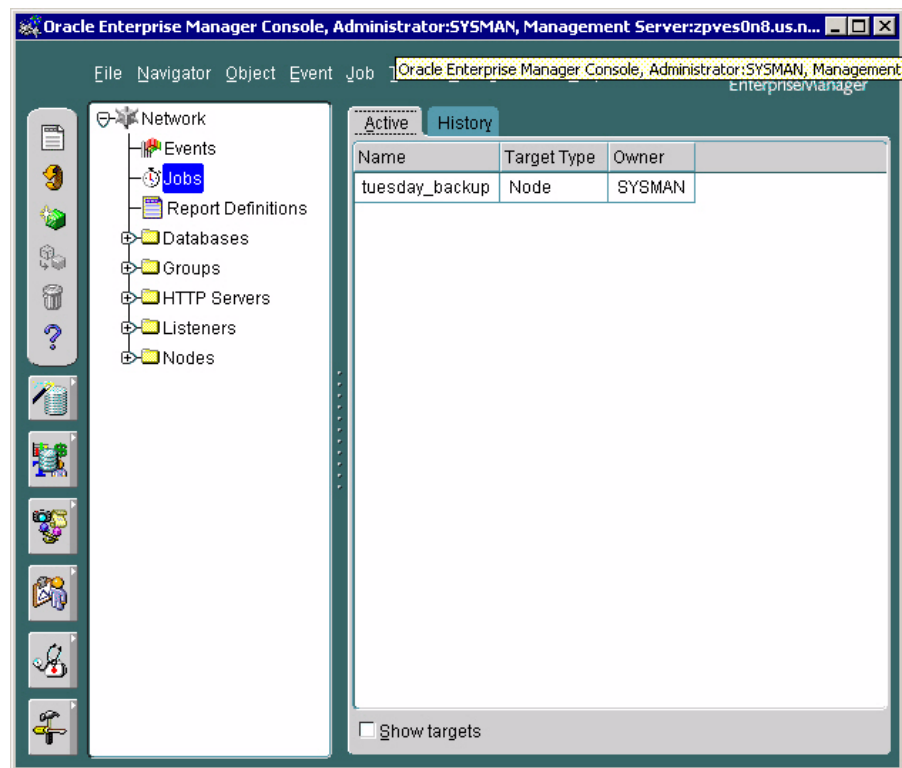
CAUTION

Only trained personnel should perform the following task.

Set general backup properties

- 1 From the **Network** tree, select **Jobs**.

The **Jobs > Active** pane displays the list of active backup jobs that have been scheduled.

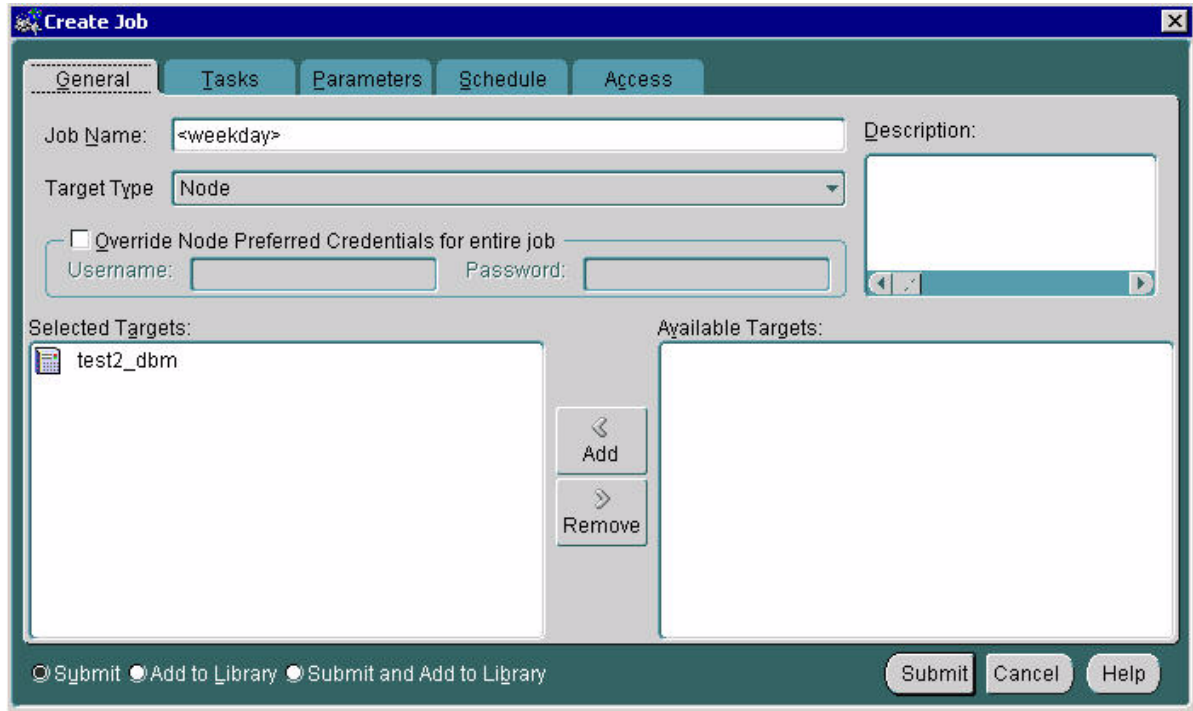


- 2 From the **Job** menu, select **Create Job**.
The **Create Job > General** pane opens.

- 3 In the **Job Name** box, type a backup name as follows:

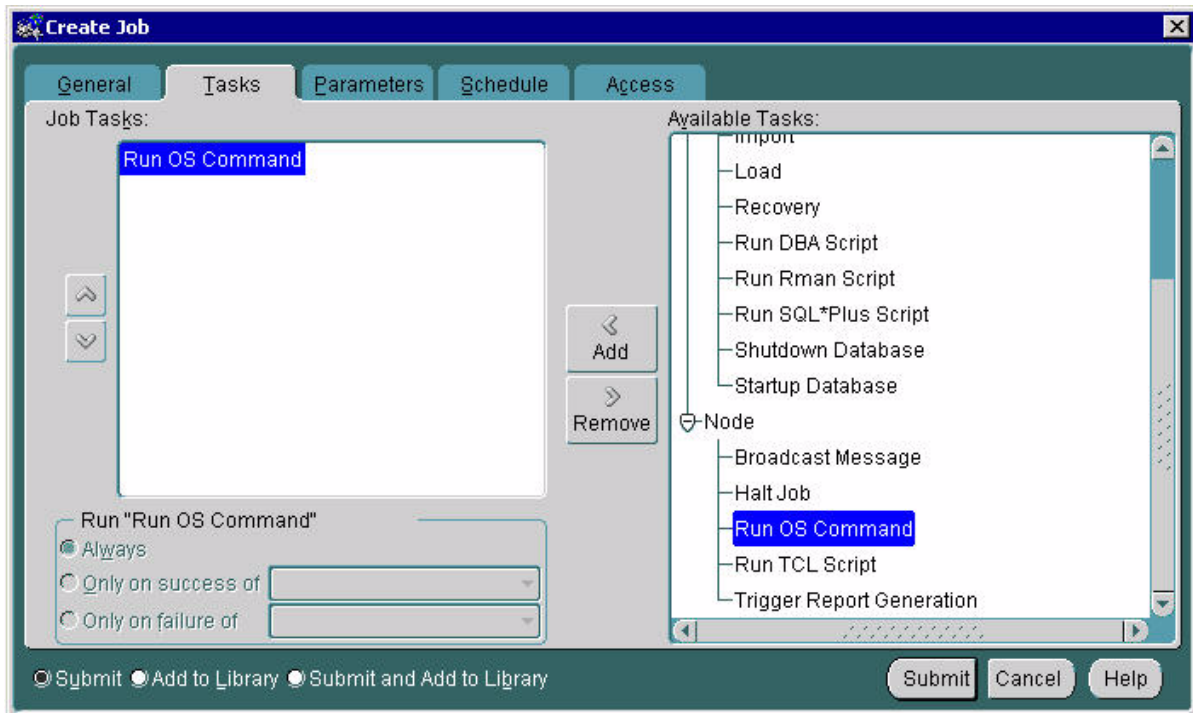
Backup type	Frequency
Export	<weekday>
Note: The Export backup method is recommended. See “Database backups” on page 71	
Alternatively, use the following backup methods:	
Level 1	level_1_backup
Level 0	level_0_backup

- 4 Under **Target Type**, select **Node**.
- 5 In the **Available Targets** box, select the node name where the Oracle server resides and click **Add**.
The selected target node moves into the **Selected Targets** list.



Set backup task properties

- 6 Click the **Tasks** tab.
The **Create Job > Task** pane opens.



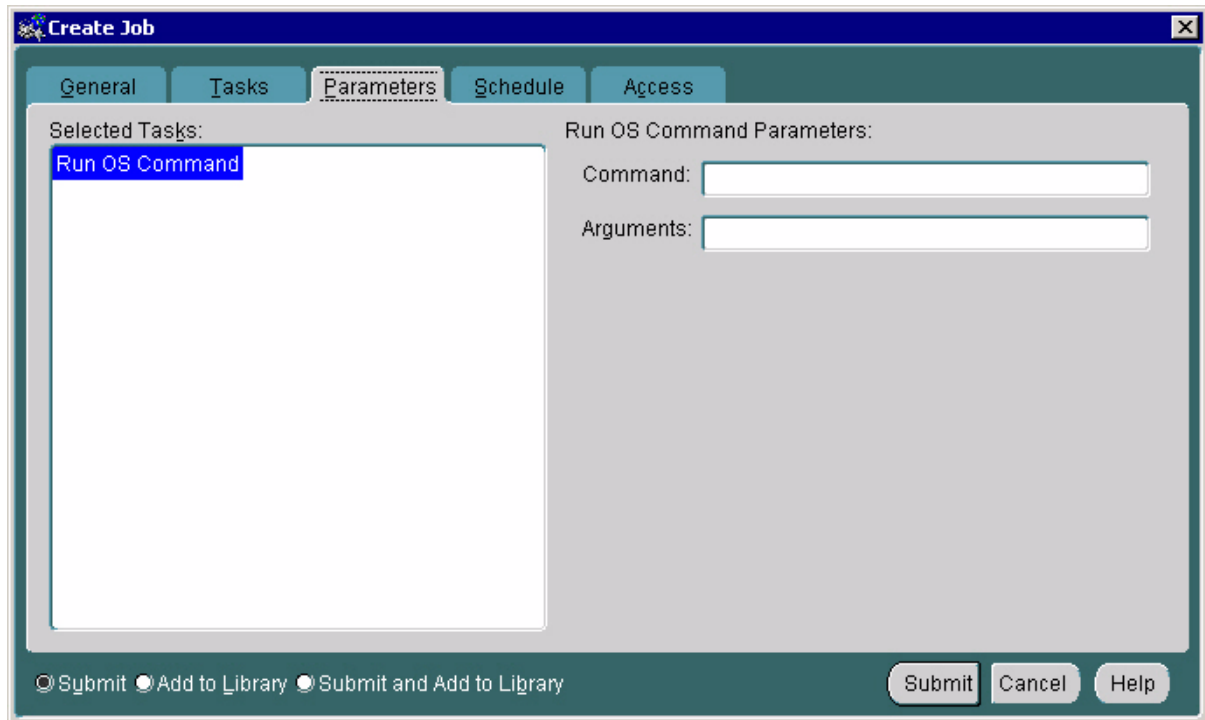
- 7 Select **Run OS command** and click **Add**.

The **Run OS command** task is added to the **Job Tasks** pane.

Define backup parameters

- 8 Click the **Parameters** tab.

The **Create Job > Parameters** pane opens.



9 In the **Command** box, enter a command as appropriate:

If	Do
Perform an Import/Export backup (recommended--see "Database backups" on page 71)	Enter the following command: /IMS/imssipdb/data/db_schema/backup/export_imsdb1.sh
Perform an RMAN full (level 0) backup	Enter the following command: /IMS/imssipdb/data/db_schema/backup/level_0_backup.sh
Perform an RMAN incremental (level 1) backup	Enter the following command: /IMS/imssipdb/data/db_schema/backup/level_1_backup.sh

10 In the **Arguments** box, enter the appropriate argument format, where **db_type** can be PRIMARY or SECONDARY,

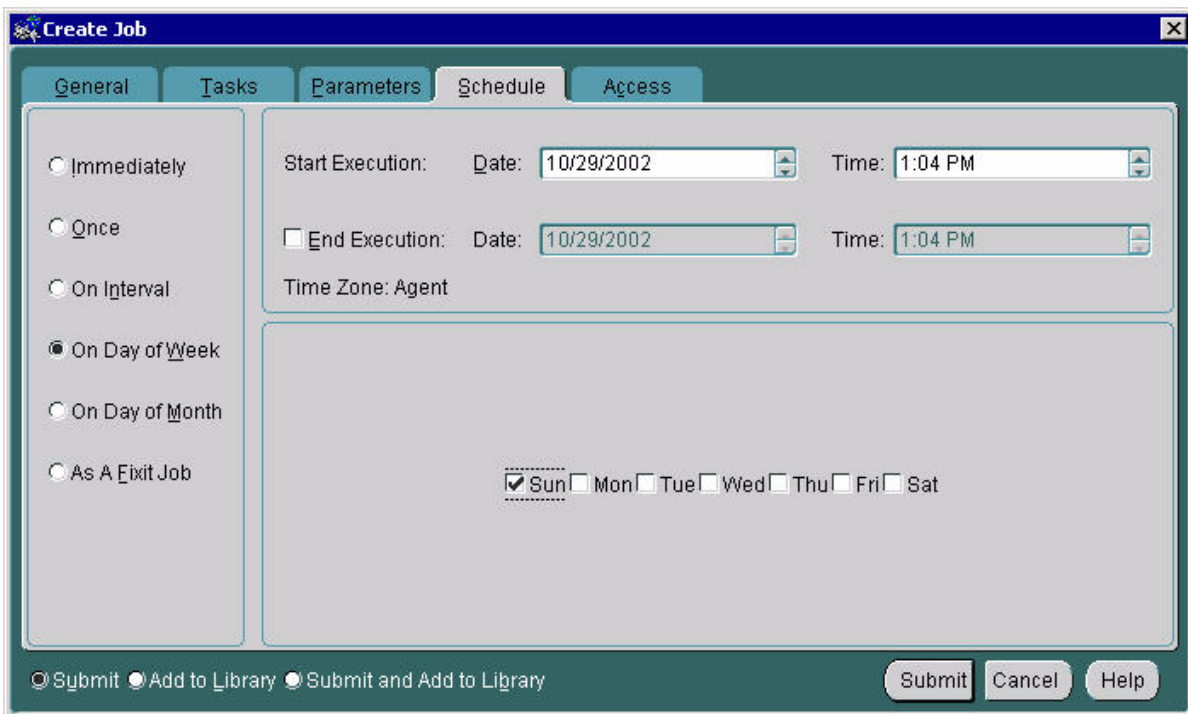
name_of_backup is the name of the backup file, and **media_type** is DISK or TAPE.

If	Do
Perform an Import/Export backup (recommended--see "Database backups" on page 71)	Use the following argument format: <db_type> <name_of_backup> <media_type>
Perform an RMAN full (level 0) backup	Use the following argument format: <db_type> <media_type>
Perform an RMAN incremental (level 1) backup	Use the following argument format: <db_type> <media_type>

Schedule backup frequency

11 Click the **Schedule** tab.

The **Create Job > Schedule** pane opens.



- 12 Do one of the following:

Note: The **Export** backup method is recommended. See “Database backups” on page 71

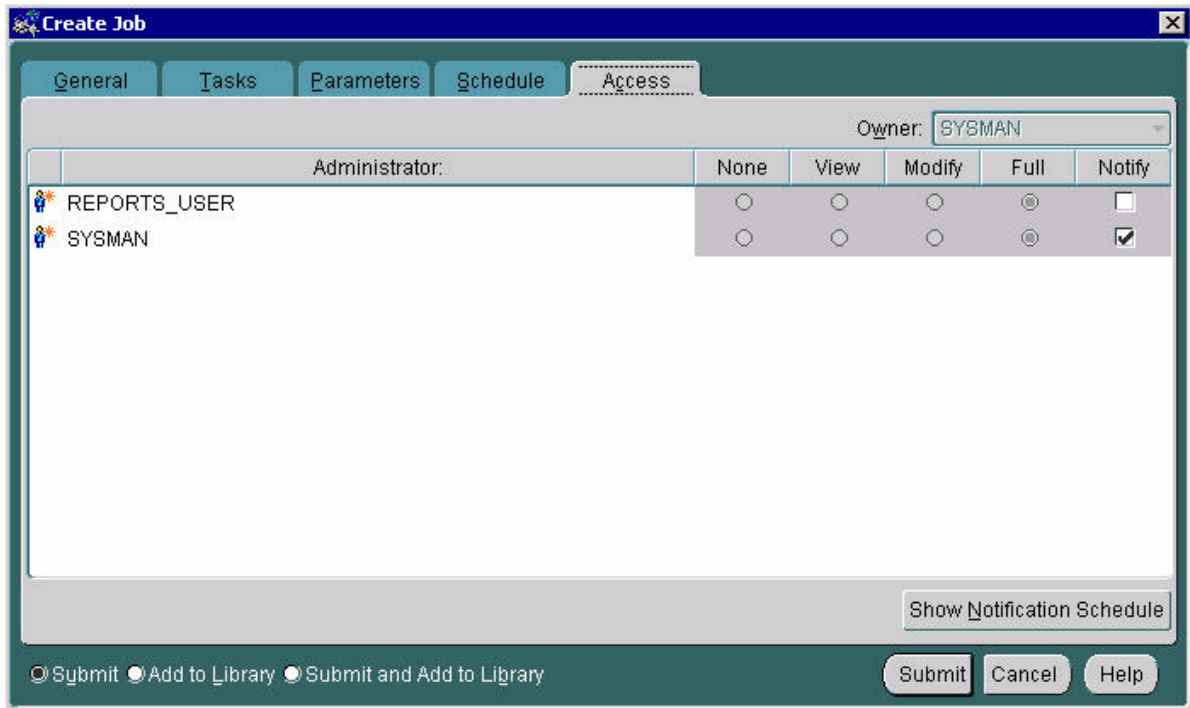
If	Do
Export backups	a. Select On Day of Week . b. Select the day of the week on which the backup should run. Note: An export backup should be created for each day of the week.
Full (level 0) RMAN backups	Select the lowest-traffic weekday (such as Sunday).
Incremental (level 1) RMAN backups	Select On Day of Week . Select the other weekdays (such as Monday through Saturday)

Note: For **RMAN** backups, full (level 0) backup jobs must be created separately and prior to incremental (level 1) backup jobs.

- 13 Choose a default start time during off-peak hours. The default time is 2:00 a.m.

Set backup notifications

- 14 Click the **Access** tab.
The **Create Job > Access** pane opens.



- 15 Make sure the **Notify** box is selected to ensure that backup reports are emailed to **SYSMAN** database administrators.

Submit and add the backup job to the library

- 16 Once all of the above steps are completed, do the following:

- a Select the **Submit and Add to Library** option.
- b Click the **Submit and Add** button to save the backup.

The **Create Job** dialog box closes and the new backup job appears in the **Active > Jobs** tab.

- 17 For **RMAN** backups, do the following:

If	Do
You first set up RMAN backups on the primary database	Backup the secondary database
You first set up RMAN backups on the secondary database	Backup the primary database

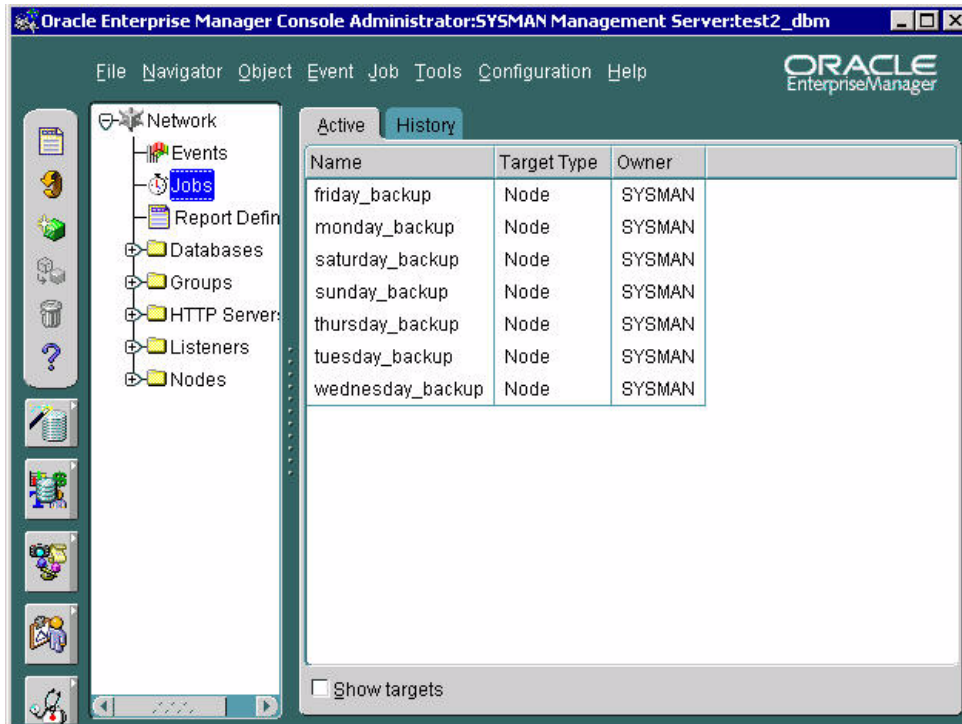
Modifying a scheduled backup job

Use the following procedure to modify scheduled backup jobs from the OEM Console.

For login instructions, see “OEM Console login” on page 45.

From the OEM Console

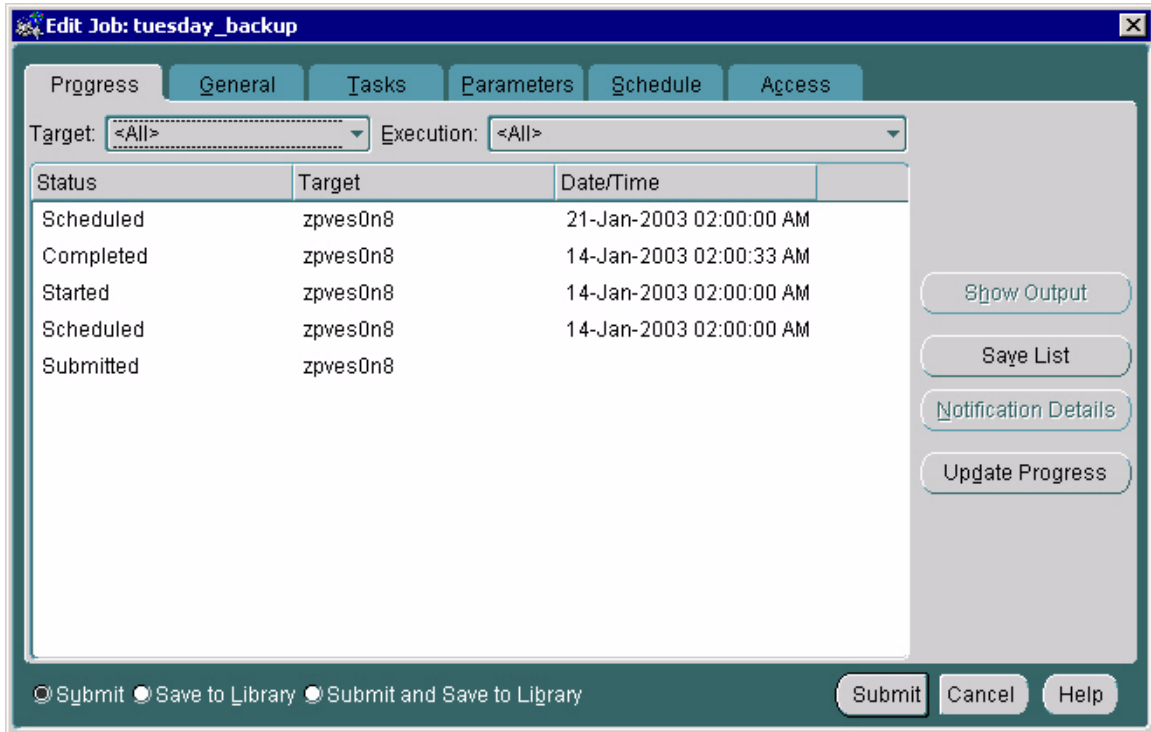
- 1 From the **Network** tree, select **Jobs**.



The **Jobs >Active** tab displays the list of active backup jobs that have been scheduled.

- 2 On the **Active** jobs panel, select the job that you want to modify.
- 3 Double-click the job name to display its properties.

The **Edit Job > Progress** tab opens.



- 4 Click any tab in the **Edit Job** dialog box to modify backup job properties.
Note: For details about appropriate backup job properties, see “Set general backup properties” on page 75.
- 5 Select **Submit and Save to Library** to save the changes to the backup job.
- 6 Click **Submit** to finish scheduling the backup job and close the dialog box.

Database recovery

This section contains the following recovery procedures:

- Restoring exported backup files
- Restoring RMAN backup files
- Restoring control files

Restoring exported backup files



CAUTION

Only trained personnel should perform the following task.

Use the following procedure to restore other files.

Note: Stop all IMS applications before performing this procedure.

On the primary database server

- 1 Shut down both the primary and secondary databases as follows:
 - a Login as **root**.
 - b Execute the following commands:
cd /etc/init.d
./dbora stop
 - c Repeat the previous step on the secondary database server.
- 2 Set up a clean database as follows:
 - a Login as **oracle**.
 - b Execute the following commands:
rm /IMS/oradata/imsdb1/*.*
cd /IMS/oradata/restore
uncompress -c emptyimsdb1.tar.Z | tar xvf -
cd /IMS/oradata/imsdb1
cp control02.ctl /opt/app/oracle/oradata/imsdb1/control01.ctl
cp control02.ctl /var/opt/oracle/imsdb1/control03.ctl
 - c Repeat the previous step on the secondary database server.
- 3 Start up the primary database as follows:
 - a Login as **root**.
 - b Execute the following commands:
cd /etc/init.d
./dbora start

- c Repeat the previous step on the secondary database server.
- 4 Restore the primary database server as follows:
 - a Login to the primary database server **oracle**.
 - b Execute the following commands:

```
cd /IMS/imssipdb/data/db_schema/backup
import_imsdb1.sh PRIMARY <name of backup>
<media_type>
```

where name of backup is the name of the backup file and media type can be a DISK or TAPE where the backup is located.
- 5 Reset replication between the primary and secondary databases as follows:
 - a Login to primary database server **oracle**.
 - b Execute the following commands:

```
cd /IMS/imssipdb/data/db_schema
single_to_rep_db.sh
```

The **single_to_rep_db.sh** script moves the data from the primary to the secondary database and sets up replication.

ATTENTION

If you use the Import/Export backup and recovery method you can restore the databases by importing the backup files from the secondary database to the primary database.

Restoring RMAN backup files**CAUTION**

Only trained personnel should perform the following task.

On the database server with the damaged files

- 1 Login as **oracle**.

- 2 To perform the recovery procedure listed in column 1, execute the commands in column 2.

Note: db_type can be PRIMARY or SECONDARY and media_type can be DISK or TAPE.

If	Do
Restore control files from a backup copy	<pre>cd /IMS/imssipdb/data/db_schema/util stop_imsdb abort cp /var/opt/oracle/imsdb1/control03.ctl /IMS/oradata/imsdb1/control01.ctl cp /var/opt/oracle/imsdb1/control03.ctl /opt/app/oracle/oradata/imsdb1/control02.ctl cd db_schema/util start_imsdb</pre>
Restore control files from disk or tape backups	<pre>restore_control_files.sh <db_type> <media_type> /IMS/oradata/imsdb1/control01.ctl</pre>
Restore the system datafile to another directory partition	<pre>restore_sys_undo_datafile.sh <db_type> <media_type> /IMS/oradata/imsdb1/system01.dbf /IMS/oradata/imsdb1/system02.dbf</pre>
Restore the undo tablespace data file to the current directory	<pre>restore_sys_undo_datafile.sh <db_type> <media_type> /IMS/oradata/imsdb1/undotbs01.dbf</pre>
Restore the undo tablespace data file to a different directory	<pre>restore_sys_undo_datafile.sh <db_type> <media_type> /IMS/oradata/imsdb1/undotbs01.dbf /IMS/oradata/imsdb1/undotbs02.dbf</pre>
Restore the IMS_DATA tablespace datafile to the same directory	<pre>restore_datafile.sh <db_type> <media_type> /IMS/oradata/imsdb1/ims_data.dbf</pre>
Restore the IMS_DATA tablespace datafile to a different directory partition	<pre>restore_datafile.sh <db_type> <media_type> /IMS/oradata/imsdb1/ims_data.dbf /IMS/oradata/imsdb1/ims_data1.dbf</pre>
Restore data files and temp tablespace	<pre>restore_temp_datafile.sh <db_type></pre>
Restore an entire database from backup	<pre>restore_database.sh <db_type> <media_type> restore_temp_datafile.sh <db_type></pre>

If	Do
Point in Time Recovery	<p>1. Execute the following command:</p> <pre>cd /IMS/imssipdb/data/db_schema/backup incomplete_restore.sh <db_type> <media_type> <TIME: YYYY-MM-DD-mm-ss> (for example, 2002-09-04:23:45:50)</pre> <p>2. Now that the PRIMARY database is restored to a point in time, look at the alert_imsdb1.log file to find the appropriate SCN.</p> <p>The alert_imsdb1.log file is located in /opt/app/oracle/admin/imsdb1/bdump/alert_imsdb1.log</p> <p>3. Edit that file and search for RESETLOGS.</p> <p>(a) If the message is, "RESETLOGS after complete recovery through change xxx," you have applied all the changes in the database and successfully performed a complete recovery. Recovery of the secondary database is not needed and this procedure is complete.</p> <p>(b) If the message is, "RESETLOGS after incomplete recovery UNTIL CHANGE xxx," you have performed an incomplete recovery. Go to the next step to complete the recovery.</p> <p>4. Record the change number from the message and enter the following commands:</p> <pre>cd /IMS/imssipdb/data/db_schema/backup incomplete_restore.sh <db_type> <media_type> SCN <scn_number></pre>

Restoring control files

Use the following procedure to restore control files.

Note: Stop all IMS applications before performing this procedure.

The examples used in this procedure assume **control02.ctl** and **control03.ctl** are damaged.

On the database server containing the damaged files

- 1 Login as **oracle**.
- 2 Change to the directory containing the **imsdb1** control files as follows:


```
cd /opt/app/oracle/admin/imsdb1/pfile
```
- 3 Open the **initimsdb1.ora** file in a text editor.
- 4 Replace the following lines:


```
control_files=("/IMS/oradata/imsdb1/control01.ctl",
```



```
/opt/app/oracle/oradata/imsdb1/control02.ctl",  
"/var/opt/oracle/imsdb1/control03.ctl")
```

with these lines:

```
control_files=("/backup/orabackup/imsdb1/control01.ctl",  
/opt/app/oracle/oradata/imsdb1/control02.ctl",  
"/backup/orabackup/imsdb1/control03.ctl")
```

- 5 Copy the **control02.ctl** and **control03.ctl** backup control files to the new location as follows:

```
cp /opt/app/oracle/oradata /imsdb1/control02.ctl  
/backup/orabackup /imsdb1/control03.ctl
```

```
cp /opt/app/oracle/oradata /imsdb1/control02.ctl  
/backup/orabackup /imsdb1/control01.ctl
```

- 6 Login to the primary database as **oracle**.
- 7 Restart the database as follows:

```
cd /IMS/imssipdb/data/db_schema/util  
stop_imsdb abort  
start_imsdb
```

Manage replication transaction errors

Replication transaction errors may result from lack of available disk space or errors in the application of queued transactions. See “Monitoring replication” on page 28.

ATTENTION

Nortel Networks recommends that you monitor error transactions once every 12 hours from the OEM Console.

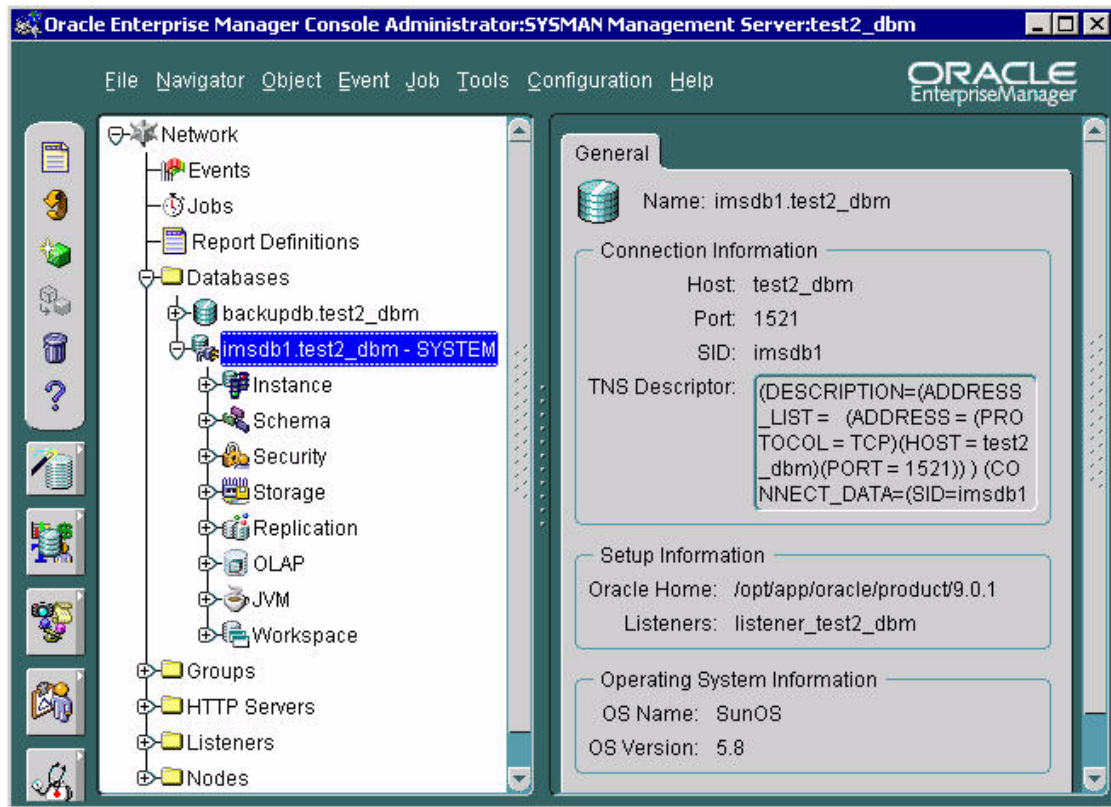
Resolving replication errors

If a replication error transaction occurs, use this procedure to resolve the conflicts.

For login instructions, see “OEM Console login” on page 45.

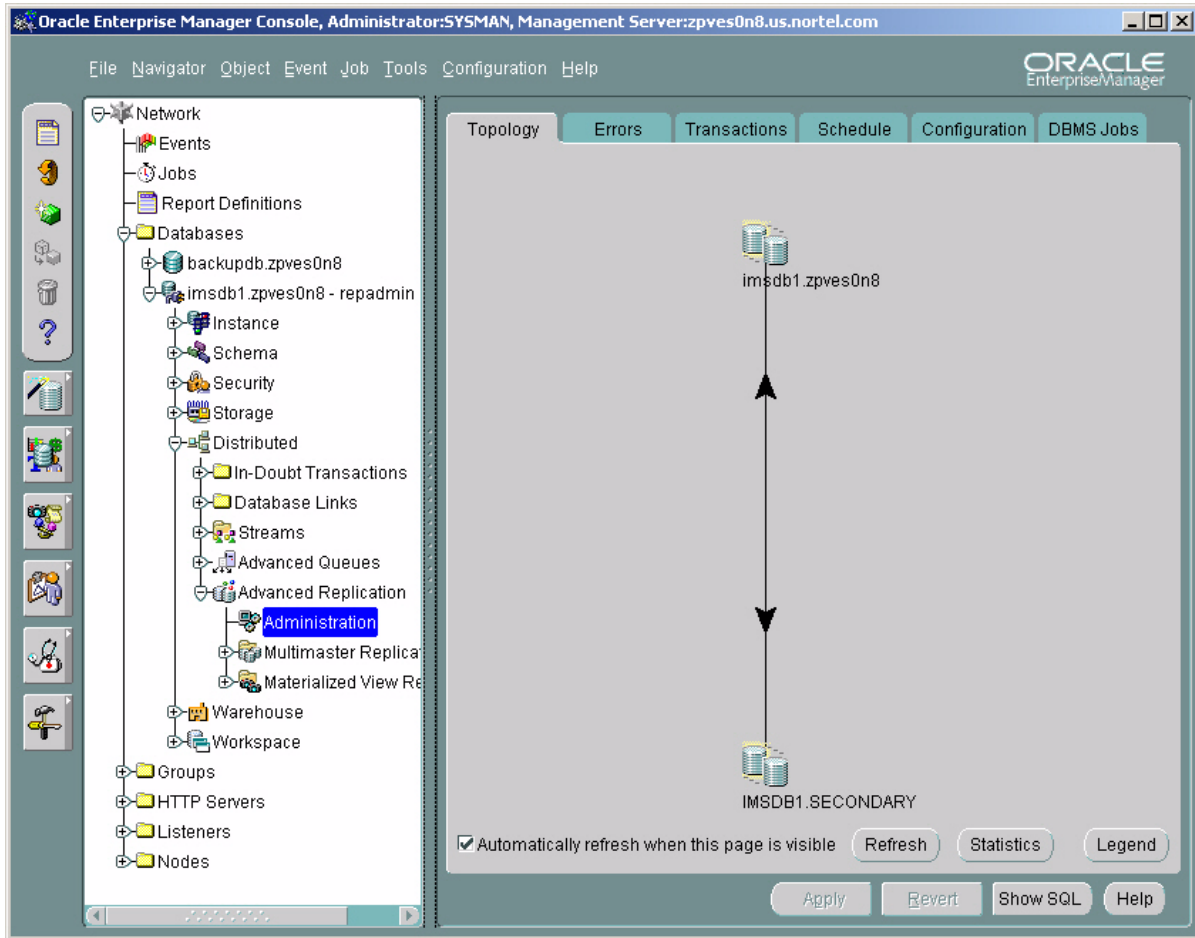
From the OEM Console

- 1 Login as **sysman**.
- 2 From the **Network** tree, select the database you want to monitor and expand the tree.



3 Select Distributed > Advanced Replication > Administration.

The **Administration > Topology** pane opens, displaying the two databases set up in replication mode.

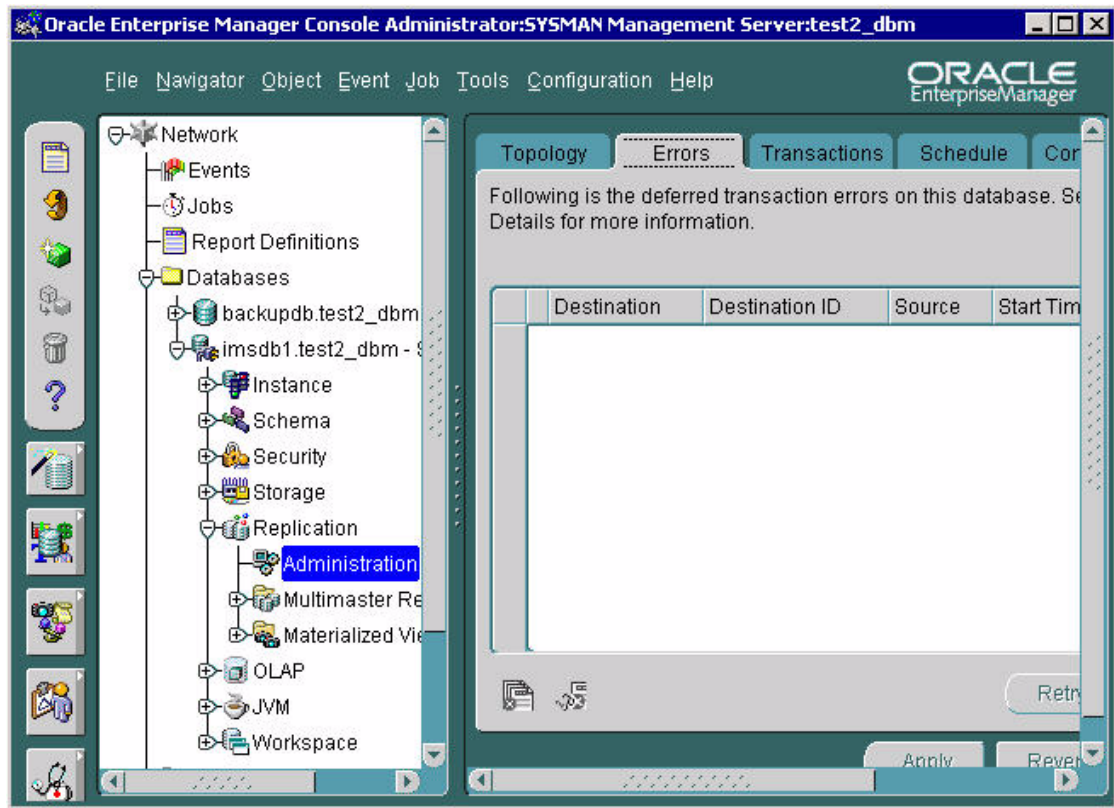


4 Click the **Errors** tab.

The **Administration > Errors** pane opens, displaying **Destination**, **Destination ID**, **Source**, **Start Time**, and **# of Calls**, where **Destination** is the primary or secondary database, **Start Time** is when the error occurred, and **# of Calls** is the number of database updates in the transaction that caused the error.

5 Click **Details** and respond as follows:

If	Do
The cause of the error is due to constraints on registration table (REGDEST)	The error can be safely deleted.
The cause of the error is NOT due to constraints on registration table (REGDEST)	Contact your next level of support for assistance.



Resynchronization

As explained in “Data replication” on page 5, the Database Module normally operates in replicated mode, wherein IMS applications write to and read from the primary database. The replication process continually propagates data from the primary database to the secondary database. The secondary database serves as a backup and therefore must remain synchronized with the primary database.

Resynchronizing databases



CAUTION

Resynchronizing databases is a lengthy process. Allow 1-2 hours to complete the operation.

Only trained personnel should perform the following task.

In the unlikely event that changes to the primary database are not propagated to the secondary database, the two databases must be manually resynchronized as follows:

In a telnet window

- 1 Login to the primary database as **oracle**.
- 2 Do the following:

```
cd /IMS/imssipdb/data/db_schema  
resync_rep_db.sh
```

Note: This command removes all application-related information from the secondary database and then resynchronizes the secondary database with the data from the primary database.

Disk space management

Oracle uses indexes to quickly access frequently used data. However, when records in a table are deleted, the associated indexes for the deleted records are nulled, but not deleted.

Over time, the indexes of frequently added and deleted tables increase in size, even though the number of records in the table stays relatively the same. Periodic optimization improves index lookup time and reduces disk usage.

The following procedure drops and recreates all the indexes in a database. It also deallocates any unused space in a tablespace, thus optimizing the space usage.

Optimizing database disk usage



CAUTION

Only trained personnel should perform the following task.

In a telnet window

- 1 Login to the primary database as **oracle**.
- 2 Navigate to the directory containing the optimization script as follows:
cd /IMS/imssipdb/data/db_schema/util
- 3 Run the optimization script by executing the following command:
optimize_dbpace.sh <db_type>

Note: **db_type** can be PRIMARY or SECONDARY.

Succession Multimedia Communications Portfolio

MCP Database Module

Basics

Copyright © 2003 Nortel Networks,
All Rights Reserved

NORTEL NETWORKS CONFIDENTIAL: The information contained in this document is the property of Nortel Networks. Except as specifically authorized in writing by Nortel Networks, the holder of this document shall keep the information contained herein confidential and shall protect same in whole or in part from disclosure and dissemination to third parties and use same for evaluation, operation, and maintenance purposes only. Changes or modifications to the MCP Database Module without the express consent of Nortel Networks may void its warranty and void the user's authority to operate the equipment.

Information is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant.

*Nortel Networks, the Nortel Networks logo, the Globemark, UNISim, Oracle, MCP, Nortel, Northern Telecom, and NT, are trademarks of Nortel Networks.

Publication number: NN10031-111
Product release: MCP 1.1 FP1 Standard
Document release: Standard MCP 1.1 FP1 (02.02)
Date: April 2003
Printed in the United States of America.

