NN10368-111

Succession

Carrier Voice over IP

Database Module Basics

(I)SN07 Standard 02.02 December 2004

NORTEL NETWORKS™

Overview

How this chapter is organized

This chapter is organized as follows:

Functional description

The Database functionality is comprised of several software components:

- Oracle database software (v9.2) - third-party software which implements basic database functionality. Administration of the Oracle database is performed through the use of the Oracle Enterprise Manager (OEM) console which is launched from the System Management Console.
- Oracle Monitor component - gathers operational status information from the Oracle database and sends it to the Management Module. This information is displayed on the System Management Console as logs, alarms and operational measurements (OMs).
- Database Module component - contains schema information for the MCS (Multimedia Communication Server) network component data. The schema information is a method of describing the MCS network component data to the Oracle database.

Architecture

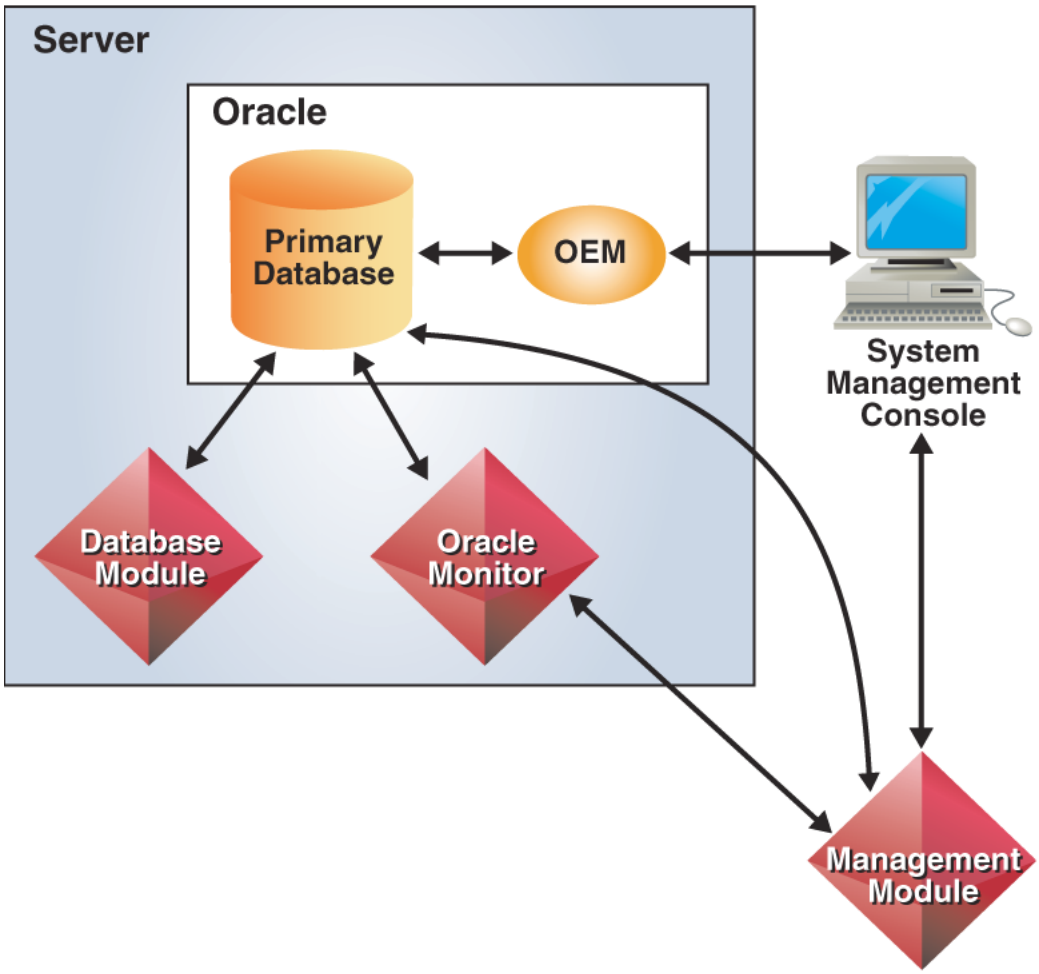
Although the normal architecture within the Carrier Voice over IP deployment is a non-redundant (simplex) database architecture, there are two different ways to architect the Database functionality based on whether redundancy is required in the network.

Non-redundant database architecture

In a non-redundant (simplex) architecture, the Database functionality is deployed on a single server. Thus, there is a single, primary, Oracle database storing the MCS network component data. In this architecture, there is no replication of MCS network component data and there is no secondary database.

A graphical representation of a non-redundant database architecture can be found in Figure 1, Non-redundant database architecture, on page 5.

Figure 1 Non-redundant database architecture

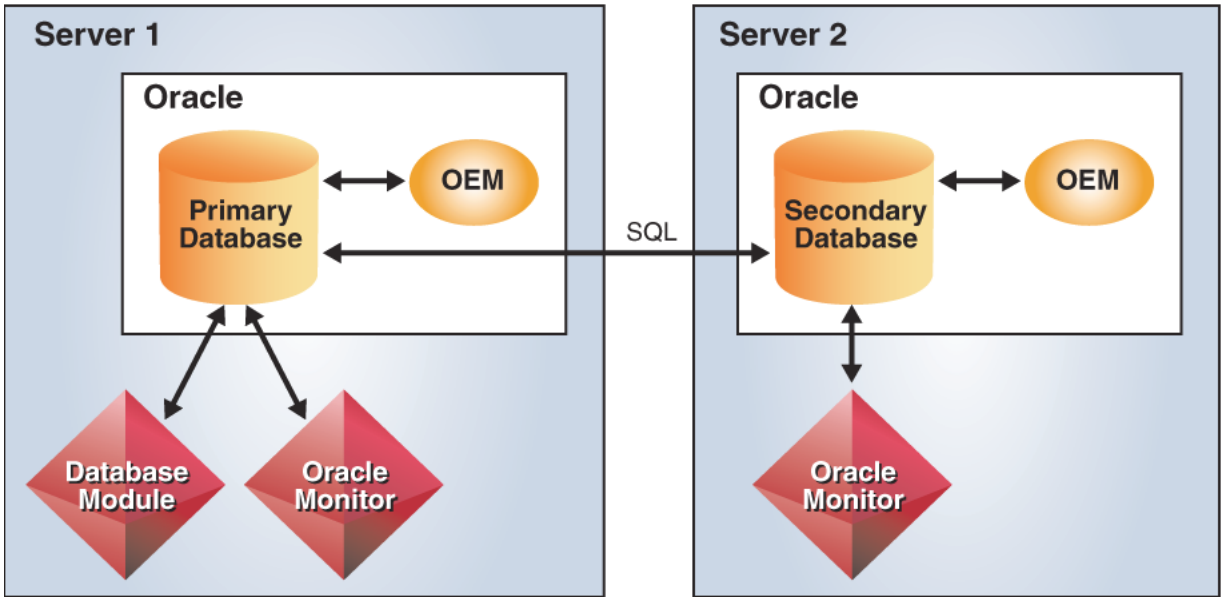


For information about the communication protocols and interactions between the server software components and other MCS network components, see Network interfaces and protocols on page 12.

Redundant database architecture

In a redundant architecture, the Database functionality is deployed similarly as it is in a non-redundant architecture, except on two servers (with an Oracle database located on each server). In this architecture, one server executes the primary database whose data is replicated to a secondary database located on the other server. Please refer to Figure 2, Redundant database architecture, on page 6 for a graphical representation.

Figure 2 Redundant database architecture



For information about the communication protocols and interactions between the server software components and other MCS network components, please refer to Network interfaces and protocols on page 12.

MCS network components normally send and receive data directly to and from the primary database. However, if an MCS network component identifies a problem with the primary database, a failover state is encountered. At this point, the MCS network component will begin to only access the secondary database to query data since the MCS network components have read-only access to the secondary database. The failover state continues until the MCS network component recognizes that the primary database has returned to service.

Database terminology

The following sections are provided to explain basic database terminology.

Replication (only in a redundant architecture)

Replication is the automatic process of duplicating data between the primary database and the secondary database as changes are received from the MCS network components.

As data is added/updated by the MCS network components, data transactions are sent to the primary database and queued for transfer to the secondary database through the Oracle replication process.

All database information is divided into groupings, called objects. Each database includes some objects which are replicated between the databases and some objects which are not replicated. Replicated objects consist only of tables. Non-replicated objects include stored procedures, functions, views, and tables.

ATTENTION
Deployment of the Database functionality creates or updates both replicated objects and non-replicated objects on both databases.

Synchronization (only in a redundant architecture)

Replicated databases should always be in synchronization due to the data transfer process described above. In the unlikely event that changes made to one database are not successfully propagated to the other database, a data transaction error (conflict) is encountered. In this case, the two databases are out of synchronization and must be manually synchronized.

For information on monitoring conflicts, please refer to Monitoring replication (only in redundant architecture) on page 41.

Database states

The Oracle database(s) have the states of operation identified in Table 1, Database operational states, on page 8. The primary

database ordinarily operates in the normal state, while a secondary database operates in a read-only state at all times.

Table 1 Database operational states

Database states	Description
Normal (Primary database)	Fully writable for the MCS network components. Inserts, updates, or deletions are permitted to the primary database. The primary database continuously transfers new data to the secondary database.
Read-only (Secondary database, only in a redundant architecture)	Read only for the MCS network components. In the unlikely event of failure of the primary database, the MCS network components failover to the secondary database. During failover, the MCS network components can only read from the secondary database. **Note:** The secondary database operates in a read-only state for the MCS network components but is always fully writable for Oracle replication processes.
Quiesced (maintenance mode)	No writes are permitted to either database. When the database is quiesced, MCS network components can only query the database and cannot insert, update, or delete information. Within a redundant architecture, the primary and secondary databases automatically enter this state whenever changes are being made to the replication environment, including modifying replication objects and synchronizing the two databases.

Database jobs

In order to help administer the Oracle database(s), jobs can be setup using the OEM console. Jobs are scripts which execute specific maintenance tasks at scheduled times, as defined within the OEM console by a database administrator.

During installation and commissioning, the following types of jobs are created:

- **Replication jobs (only in a redundant architecture):**
  - **Push Job:** used to reassign all data transactions in the queue to the other database. This type of job is scheduled every 30 seconds.
  - **Purge Job:** used to delete all transactions in the queue that have been transferred to the other database. This type of job is scheduled every 10 minutes.

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

Database backup and recovery

The Database functionality supports the ability to backup the Oracle database using the OEM Console. It is recommended that the Export/Import backup method be used. For more information regarding this backup method, please refer to Database backup on page 101.

ATTENTION

It is also recommended that the Oracle database be backed up daily whether it is a redundant configuration or not. If there is no redundancy in the network, there is no replication process, thus a backup of the data is even more important.

Recovery of an Oracle database restores the database to the last point in time when the database (or secondary database within a redundant architecture) was backed up. All changes made to the database since that last point in time will be lost.

Events

Database administrators use the OEM Console in order to register database events for monitoring. As the database events are encountered, alerts are generated and displayed on the OEM Console.

Alert log files and trace files

Other database status information is stored in an alert log file for the corresponding Oracle database. This file holds a chronological log of messages and errors, such as all internal errors, block corruption errors, and deadlock errors.

In addition to the alert log file, when an Oracle process detects an error, it dumps detailed information about the error into a trace file.

Tablespaces

Tablespaces are entities which hold table information (MCS network component and Oracle data in the form of tables). Tablespaces are allocated a certain amount of disk space.

ATTENTION

It is recommended that tablespaces be regularly monitored from the OEM Console to ensure that they do not run out of disk space. In cases where a Critical alarm is raised at the System Management Console regarding the exceeding of the disk threshold for the /IMS partition on the server hosting the primary database (or secondary database, in a redundant architecture), it is recommended that the tablespaces sizes/usage be examined via the OEM console. For information on how to perform this monitoring, please refer to Monitoring tablespace usage on page 40.

Reports

The OEM Console can generate reports about configuration, status, events, and backup jobs as required.

Hardware

The Database functionality is deployed on Sun Netra 240, Sun Fire V240, or Sun Fire V100 server(s). The following table gives a highlevel description of the hardware details of the hosting servers.

Table 2 Management Module hosting hardware

Hardware	Details
Sun Fire V240 or Sun Netra 240  Although essentially the same, the Sun Fire V240 is AC powered, whereas the Sun Netra 240 is DC powered.	Both the Sun Fire and Netra 240 servers have the following hardware features: • 2 x 1.2 GHz UltraSPARC IIIi processors • 4 GB RAM • 1MB Internal Cache • 2 x 73GB hard disks • 1 x internal DVD-ROM Drive • 4 x 10/100/1000 Base-T Ethernet Ports • 2 x USB Ports • 2 x Serial Ports
Sun Fire V100 	The server has the following hardware features: • 1 x 650 MHz UltraSparc IIi processor • 1 GB RAM • 512 Kb on-chip L2 cache • 2 x 40 GB hard disks • 2 x 24x internal CD-ROM • 2 x 10/100 Base-T Ethernet ports • 2 x USB ports • 2 x Serial ports

Note: In a redundant architecture, two servers are required for managing the two Oracle databases (primary and secondary).

Server backup and recovery

There are capabilities to back up and recover Multimedia Communication Server (MCS) server software and hardware as a result of specific hardware failures. These capabilities range from the ability to recover the hardware and software after minor server failures

to the recovery of hardware and software after catastrophic server failures.

Backups of MCS servers are recommended in order to recover from a catastrophic failure where a complete restore of the server's software (both third party and component software) and server configuration information is required.

ATTENTION

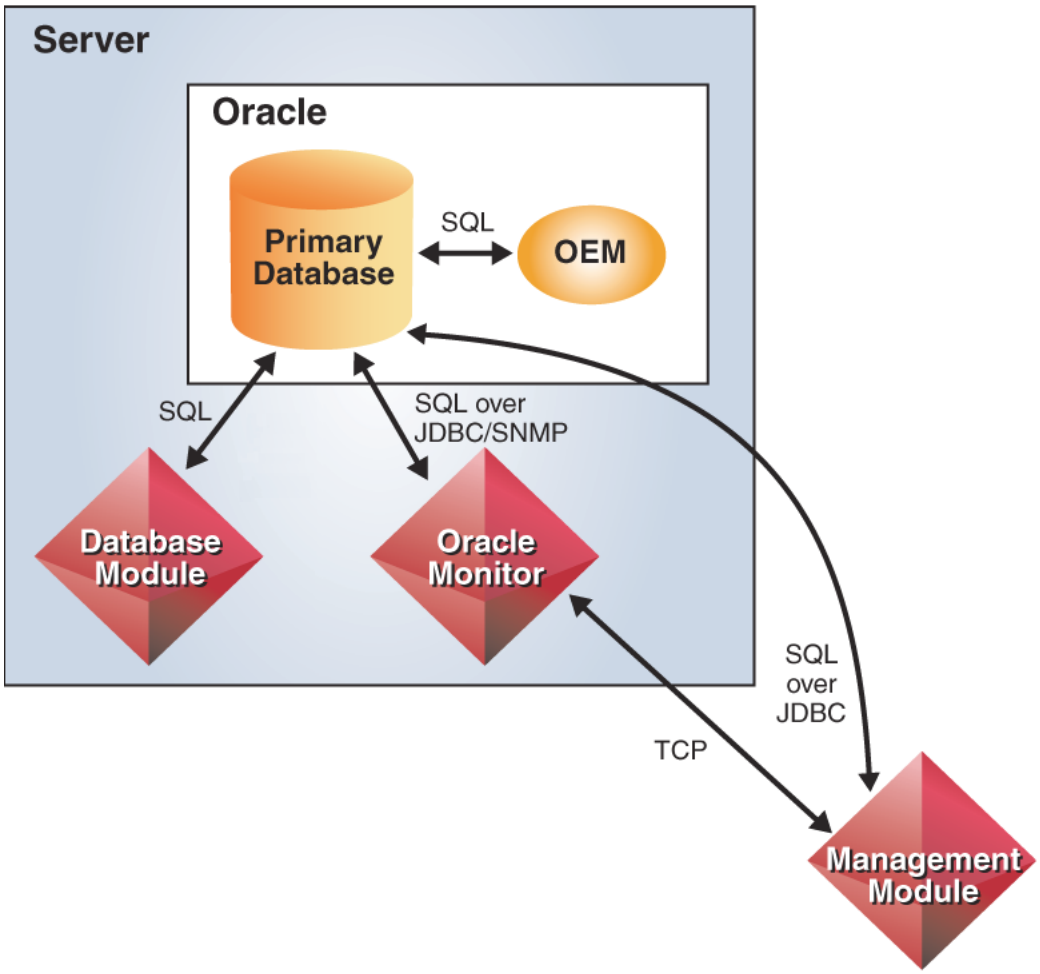
Backups of the MCS servers are highly recommended in certain situations based on the software resident on the server. These situations include when the Solaris Operating System on any MCS server is updated, the Oracle software on the server running the Oracle database is updated, and when an MCS software maintenance release for the Management Module is deployed to a server.

Please refer to the *MCS Backup and Recovery Guide* for details regarding backup and recovery procedures for MCS servers.

Network interfaces and protocols

Network interfaces connect to the Database functionality on the server as shown in Figure 3, Network interfaces to Database functionality, on page 13.

Figure 3 Network interfaces to Database functionality



These network interfaces connect to the software applications and MCS network components on the server using the following protocols:

- **Structured Query Language (SQL):** The Oracle database(s) use SQL in order to communicate with the OEM console and with another Oracle database when using a redundant database architecture.
- SQL over Java Database Connection (JDBC): The Oracle database(s) communicates with MCS network components using SQL over JDBC.

- **Simple Network Management Protocol (SNMP):** The Database functionality uses SNMP in the following areas:
  - The server hosting the database uses an SNMP agent in order to provide operational information for the server to the Management Module component.
  - The Oracle Monitor component uses an Oracle SNMP agent to gather Oracle database state information.
- **Transmission Control Protocol (TCP):** TCP is used to communicate configuration, performance data, logs, and alarms between the Oracle Monitor component and the Management Module.

Tools and utilities

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

- **System Management Console:** Launches the OEM Console, deploys the Oracle Monitor component, and updates the Database Module and Oracle Monitor components. Provides operational, fault, and state information for the Oracle database through the Oracle Monitor component. For more details, please refer to *CVoIP System Management Console User Guide*.
- **Oracle Monitor Component:** Gathers operational status of an Oracle database and sends logs, alarms and operational measurements (OMs) to the Management Module to be displayed on the System Management Console. The tool uses the Oracle SNMP agent to gather information about tablespace utilization and other database information.
- **Oracle Enterprise Manager (OEM) Console:** Used by the database administrator for fault management of the Oracle database and the administration of database related events and jobs.

OAM&P strategy

Off-line data migration between releases and maintenance updates are supported. For more information, please refer to Off-line migration on page 17.

Database backup and recovery are also supported.

Tasks

After installation and commissioning, an upgrade involving the upgrade of the Oracle software, or the restoration/recovery of the Oracle database(s), it is recommended that certain configuration and administration tasks are performed.

Table 3, Database functionality task flows, on page 15 outlines the tasks recommended for the Database functionality.

Table 3 Database functionality task flows

Topic	Subtopic	Procedure
Configuration	**sysman** preferences	Configuring sysman preferences on page 76
	Read-only user	Configuring a database observer account on page 79
Administration	Registering/Scheduling Events	Creating an Oracle database event on page 104
	Export/Import backups	Creating an Export/Import Oracle database backup job on page 109

Legal note

All basic operations of the Oracle programs which are embedded in the Database functionality, including but not limited to database management operations, must be managed from within Nortel Networks software components and Graphical User Interfaces (GUIs).

Upgrades

How this chapter is organized

This chapter is organized as follows:

Functional description

Deployment of Database functionality

The following deployment tasks related to the Database functionality are performed during installation and commissioning or when upgrading to a full release:

- Addition and configuration of the server(s) hosting the Database functionality.
- Installation of Oracle onto the server(s), including the creation of the **oracle**, **sysman**, and **system** administrator accounts.
- Addition and configuration of the Database Module software component onto the server hosting the primary database

  Note: In a redundant architecture, the Database Module component is not deployed on the server hosting the secondary database. When an update is made to the Database Module component on the server hosting the primary database, the new schema information is communicated to the secondary database.

This chapter documents upgrade tasks that can be performed when upgrading to a maintenance release. For information on upgrading to a full release, please contact your next level of support.

Off-line migration

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

Once the Database Module is upgraded to a new release, the Database functionality can be upgraded to future maintenance releases using the update functionality within the System Management Console. As part of this process, the system automatically creates a backup of the existing Oracle database, assigning a backup name that contains the release name. That backup is then available, if necessary, to restore the Database Module and Oracle database to an earlier release.

Tools and utilities

Maintenance updates (both upgrades and downgrades) to the Database Module and Oracle Monitor components are performed through the use of the System Management Console. The only exception being the rollback/downgrading of the Database functionality in a redundant architecture. For more information, refer to Rollback/Downgrade of the Database Module in a redundant architecture on page 23.

The update operation on the System Management Console allows administrators to either upgrade the Database Module or Oracle Monitor component to future maintenance releases, or downgrade these components to a previous maintenance release.

OAM&P strategy

Database Module

In a non-redundant network, an upgrade failure results in an automatic rollback to the previous load.

In a redundant network, an upgrade failure does not result in an automatic rollback due to the amount of time the database would be in a quiesced state (making both the primary and secondary database unavailable to the MCS network components for write access). In this scenario, the administrator must perform a manual rollback to the previous load as described in Rollback/Downgrade of the Database Module in a redundant architecture on page 23.

Oracle Monitor

If an upgrade fails before or during the initial stages of the upgrade, a rollback to the previous load is performed. A notification of the failure appears within the System Management Console. If a component upgrade fails after the initial stages of the upgrade, it does not roll back automatically. A dialog box appears stating the upgrade failed and prompts the administrator to determine whether a rollback should be performed.

Tasks

Table 4, Upgrade/Downgrade task flows, on page 19 outlines upgrade/downgrade procedures for the Database functionality.

Table 4 Upgrade/Downgrade task flows

Topic	Sub-topic	Procedure
Database Module component	Upgrading	Updating the Database Module software load on page 20
	Downgrading (in a non-redundant architecture)	Updating the Database Module software load on page 20
	Rollback/Downgrading (in a redundant architecture)	Rollback/Downgrade of the Database Module in a redundant architecture on page 23
Oracle Monitor component	Upgrading/Downgrading	Updating the Oracle Monitor software load on page 25
Oracle database	Upgrading from a non-redundant architecture to a redundant architecture	Upgrading to include a redundant database on page 27

Updating the Database Module component

The update operation on the System Management Console allows administrators to either upgrade the Database Module component to

future maintenance releases, or downgrade the Database Module component to a previous maintenance release.

Note: Rollbacks/Downgrades of the Database Module are only successful when downgrading to a previously running maintenance release.

CAUTION

The ability to revert the Database Module component back to a previous version is provided as a fail-safe mechanism. This functionality should never be used under normal circumstances.

When the Oracle 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 downgrading the Database Module component to a previous version.

Database Module maintenance updates include database schema files, stored procedures, and backup/recovery scripts.

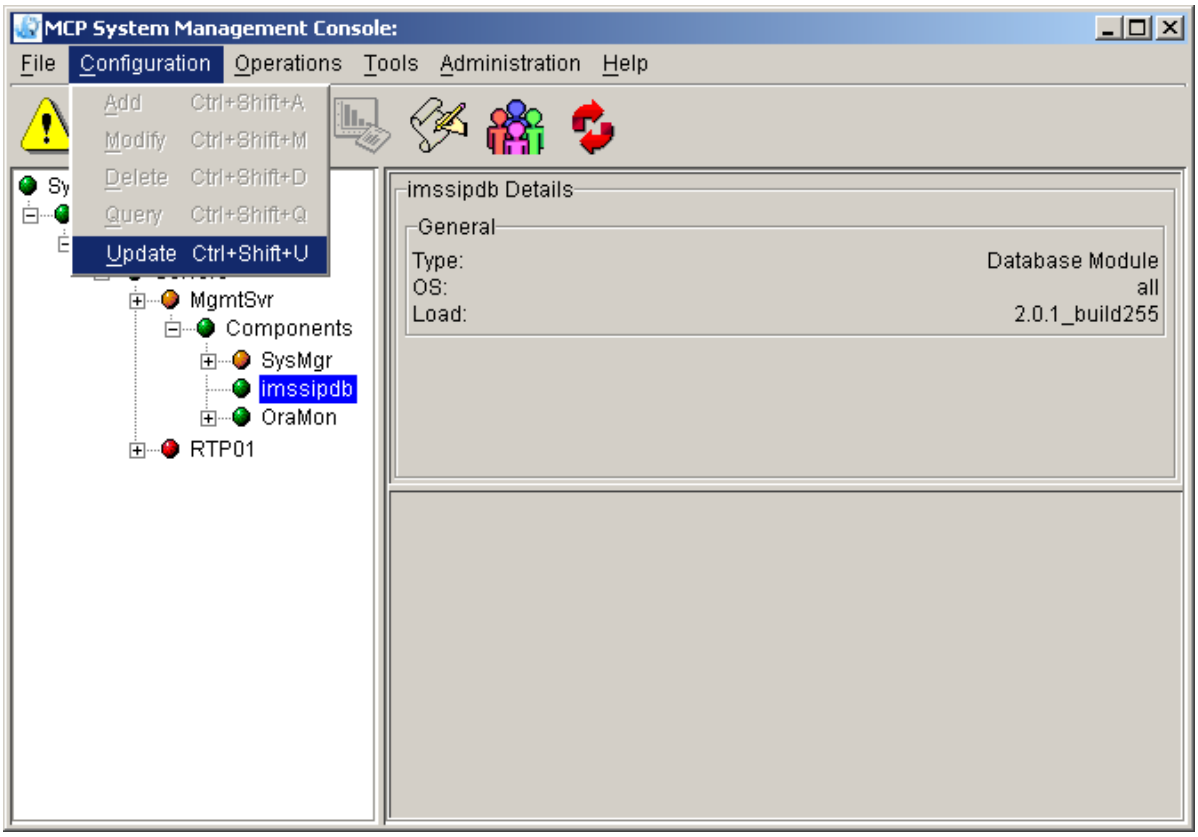
Maintenance updates (except for the rollback/downgrade of the Database Module in a redundant architecture, refer to Rollback/Downgrade of the Database Module in a redundant architecture on page 23) should be performed as described in the following procedure:

Updating the Database Module software load

From the System Management Console

1. In the System tree, select the Database Module component (**imssipdb**).
2. From the Configuration menu, select the **Update** command.

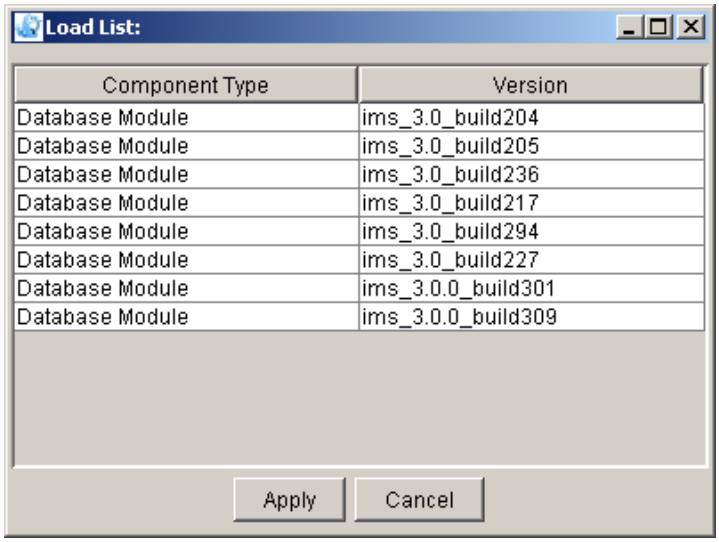
Figure 4 Update from the Configuration menu



You can also launch the update command by right-clicking on the Database Module component and selecting **Update** from the pop-up menu.

3 After **Update** is selected, the Load List window appears. The window only shows software loads intended for the Database Module component type, since this is the component type being updated.

Figure 5 Load list for updating



4 Select the load version that should be used to update the Database Module component. Click on the **Apply** button.

When downgrading to a previous running version of the Database Module component, the administrator is warned that doing so removes data gathered since installation/previous update.

The appropriate database scripts are copied onto the server hosting the Database Module and primary database. In addition, the Oracle database(s) is updated to the schema corresponding to the Database Module load selected.

Rollback/Downgrade of the Database Module in a redundant architecture

If a failure occurs during the upgrade process for any MCS network component, an automatic rollback is usually performed. An indication of this automatic rollback is displayed on the System Management Console. However, when an upgrade failure is encountered for the Database Module in a redundant architecture, an automatic rollback is not performed. It is recommended, in order to limit downtime, that the procedures in this section be manually performed.

The same manual procedures used to rollback the Database Module to a previous maintenance release are used to downgrade the Database Module as well. However, these steps are used within a larger process in order to achieve limited downtime.

CAUTION

Any MCS network components which were upgraded after the last deployment/upgrade of the Database Module component will also require a downgrade. Please contact your next level of support.

Downgrade the Primary database

Drop replication between the primary and secondary databases:

1 Log in as **oracle** to the server hosting the primary database.

2 Execute the following commands:

cd /IMS/imssipdb/data/db_schema/util

./remove_replication.sh

Deploy the downgraded load version of the Database Module to the server hosting the primary database:

1 Log in as **nortel** to the server hosting the active Management Module component.

2 Execute the following commands:

cd /opt/sb/dsm2/bin

./**dbdeploy.pl**

where the database is being deployed as a single database and the type of deployment is **Rollback**.

Update information to show that the primary database is

replicated:

1 Log in as **oracle** to the server hosting the primary database.

2 Execute the following commands:

cd /IMS/imssipdb/data/db_schema

3 Edit the **define.sql** file by changing the IP address in the following line:

define db2_ip_address = <IP_Address>

where **IP_Address** is the IP address of the secondary database.

Downgrade the Secondary database and setup replication

Prepare for replicating databases:

1 Log in as **oracle** to the server hosting the primary database.

2 Execute the following commands:

cd /export/home/oracle/bin/upgrade/logs

pwd (verify that path displayed is the same as path listed in above **cd** command)

rm *

cd /export/home/oracle/bin/upgrade

./prepare_replication.sh

when prompted to restart the database, type **Y**.

Backup primary database and start queueing data transactions:

1 Log in as **oracle** to the server hosting the primary database.

2 Execute the following commands:

cd /export/home/oracle/bin/upgrade

./add_secondary_db.sh

Activate the secondary database

1 Log in as **oracle** to the server hosting the secondary database.

2 Execute the following commands:

cd /export/home/oracle/bin/upgrade

./activate_secondary_db.sh <primary_DB_hostname>

when prompted to restart the database, type **Y**.

Turn off archiving logs on primary database:

1 Log in as **oracle** to the server hosting the primary database.

2 Execute the following commands:

cd /export/home/oracle/bin

./archivallogctl off

when prompted to restart the database, type **Y**.

Clean up the primary and secondary databases:

1 Log in as **oracle** to the server hosting the primary database.

2 Execute the following commands:

cd /export/home/oracle/bin/upgrade

./clean.sh

Note: The clean.sh script removes logs and files that were used temporarily during the rollback. This command does not alter any data in the database.

3 Repeat this procedure on the server hosting the secondary database.

Updating the Oracle Monitor component

The update operation on the System Management Console allows administrators to either upgrade the Oracle Monitor component to a maintenance release, or downgrade the Oracle Monitor component to a previous maintenance release.

Maintenance updates should be performed as described in the following procedure:

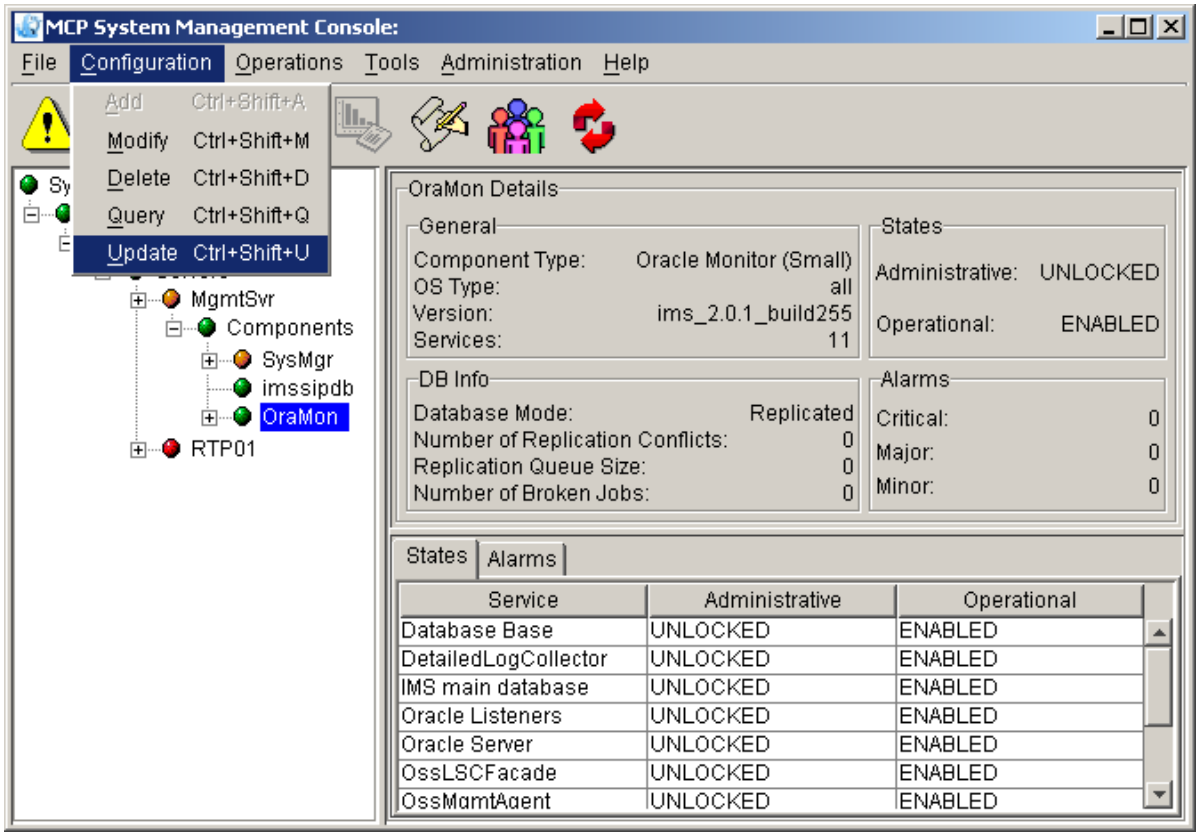
Updating the Oracle Monitor software load

From the System Management Console

1 In the System tree, select the appropriate Oracle Monitor component.

2 From the Configuration menu, select the **Update** command.

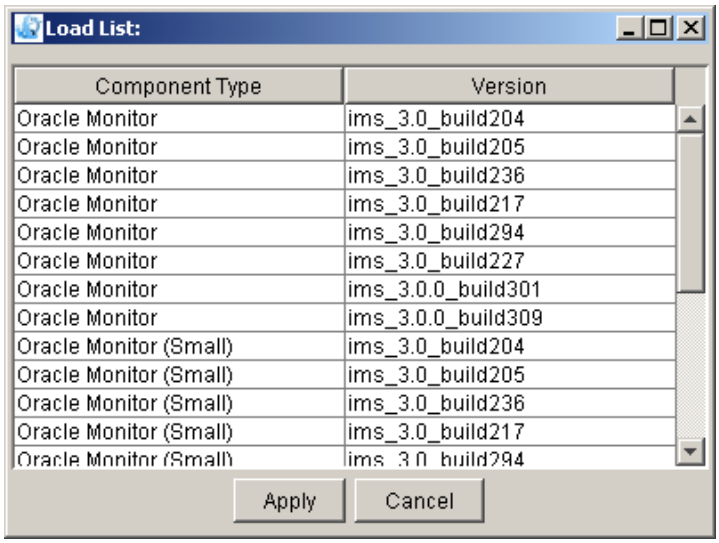
Figure 6 Update from the Configuration menu



You can also launch the update command by right-clicking on the Oracle Monitor component and selecting **Update** from the pop-up menu.

3 After **Update** is selected, the Load List window appears. The window only shows software loads intended for the Oracle Monitor component type, since this is the component type being updated.

Figure 7 Load list for updating



4 Select the load version that should be used to update the Oracle Monitor component. Click on the **Apply** button.

5 You will be prompted to configure the Oracle Monitor configuration tabs and properties.

Note: It is recommended that all of the default configuration values be used when updating the Oracle Monitor component.

6 Click on the **Apply** button. A window showing the progress of the update appears.

7 Once the update has completed, a window appears showing that the Oracle Monitor component was successfully updated.

8 In a redundant architecture, repeat this procedure to add the Oracle Monitor component to the server hosting the secondary database.

Upgrading to include a redundant database

To expand and upgrade an MCS network from a non-redundant database architecture (in other words, a single, primary database) to a redundant database architecture, a secondary database (located on a separate server than the primary database) is added. The existing primary database must be transformed into a replicated database by performing the resynchronization process. The process for resynchronizing a replicated database is provided in Resynchronizing (from Primary to Secondary) on page 1.

Fault management

How this chapter is organized

This chapter is organized as follows:

Functional description

Fault management for the Database functionality consists of monitoring and responding to information provided by the System Management Console (via the Oracle Monitor component) and the Oracle Enterprise Manager (OEM) Console.

To provide a recovery mechanism for a fault scenario, the Oracle database(s) should be backed up on a regular basis. For backup and recovery procedures, see Administration on page 99.

CAUTION

It is recommended that the Oracle database(s) and external backup media be maintained in separate locations to prevent data loss in case of natural disaster, security breech, or other unforeseen event.

Database failover in a redundant architecture

In addition, a redundant architecture provides the ability for data to be replicated across Oracle databases. As updates are applied to the primary database, they are transferred to the secondary (replicated) database. In the unlikely event of a failure of the primary database, MCS network component queries are redirected to, that is, “failover” to the secondary database.

During a failover, MCS network components periodically attempt to access the primary database. Once the primary database returns to service, all data processing reverts to the primary database.

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

- Raises a major alarm indicating a problem with the primary database
- Switches over to the secondary database and re-initiates the request

ATTENTION

A critical alarm is raised on the System Management Console when MCS network components are not able to connect to both the primary and secondary databases.

A minor alarm is raised on the System Management Console when MCS network components are connected to the primary database and the connection to the secondary database fails.

If all the associated alarms are cleared, then the MCS network components are accessing the primary database.

Events

As registered database events occur, alerts are raised and written to file in order to notify the database administrator that the event was encountered. For more information on how to register database events, refer to Registering an Oracle database event on page 104.

When a registered event is encountered, an alert displays on the OEM Console. Alerts have progressively higher severity levels as shown in the following table.

Alert Severity	Icon description	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.

Alert Severity	Icon description	Description
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.

Tools and utilities

Use the following tools to perform fault monitoring for the Database functionality:

- **System Management Console:** provides logs and alarms for the Oracle database(s) through the Oracle Monitor component(s). For information on monitoring and responding to fault information within the browsers of the System Management Console please refer to *CVoIP System Management Console User Guide*.

  Note: The System Management Console does not display any logs or alarms or logs for the Database Module component.

- **Oracle Monitor component:** Gathers status information for an Oracle database. This information is analyzed and appropriate logs and alarms are sent to the Management Module to be displayed on the System Management Console. The tool uses the Oracle SNMP agent to gather information about tablespace utilization and other database information.
- **Oracle Enterprise Manager (OEM) Console:** provides the status of database jobs, alert information, and disk usage.

Tasks

Table 5, Fault management task flows, on page 32 outlines fault management tasks for the Database functionality.

Table 5 Fault management task flows

Topic	Subtopic	Procedure
System Management Console Monitoring	Oracle Monitor component	Oracle Monitor component on page 33
Oracle Enterprise Manager Console Monitoring	Backup jobs	Monitoring database backup jobs on page 35
	Events and Alerts	Monitoring alerts on page 38
	Tablespace usage	Monitoring tablespace usage on page 40
	Replication (only in a redundant architecture)	Monitoring replication (only in redundant architecture) on page 41
	Replication Conflicts (only in a redundant architecture)	Resolving data transaction errors (only in a redundant architecture) on page 43
	Replication jobs (only in a redundant architecture)	Monitor replication jobs (only in redundant architecture) on page 45
Server Monitoring	Alert logs and trace files	Monitoring alert log files and trace files on page 48

Table 5 Fault management task flows

Topic	Subtopic	Procedure
	Undo tablespace resizing	Resizing the Undo tablespace on page 48
	Resynchronization (only in a redundant architecture)	Resynchronization (only in a redundant architecture) on page 49

System Management Console Monitoring

The majority of faults for the Database functionality are monitored on the System Management Console only after the Oracle Monitor component is deployed. The administrator must deploy the Oracle Monitor component(s) for the Oracle database(s). The Oracle Monitor component uses SNMP agents and SQL queries to monitor it's corresponding Oracle database. After analyzing the data it has collected, the Oracle Monitor component sends information to the Management Module to be displayed on the System Management Console in the form of logs, alarms, and operational measurements (OMs).

Oracle Monitor component

On the System Management Console, the Oracle Monitor component provides alarm and log information about the following areas:

- the **IMS main database** (see IMS Main Database tab on page 69)
- the **Oracle Server** (see Oracle Server tab on page 71)
- **Oracle Listeners** (see Oracle Listener tab on page 71)

ATTENTION

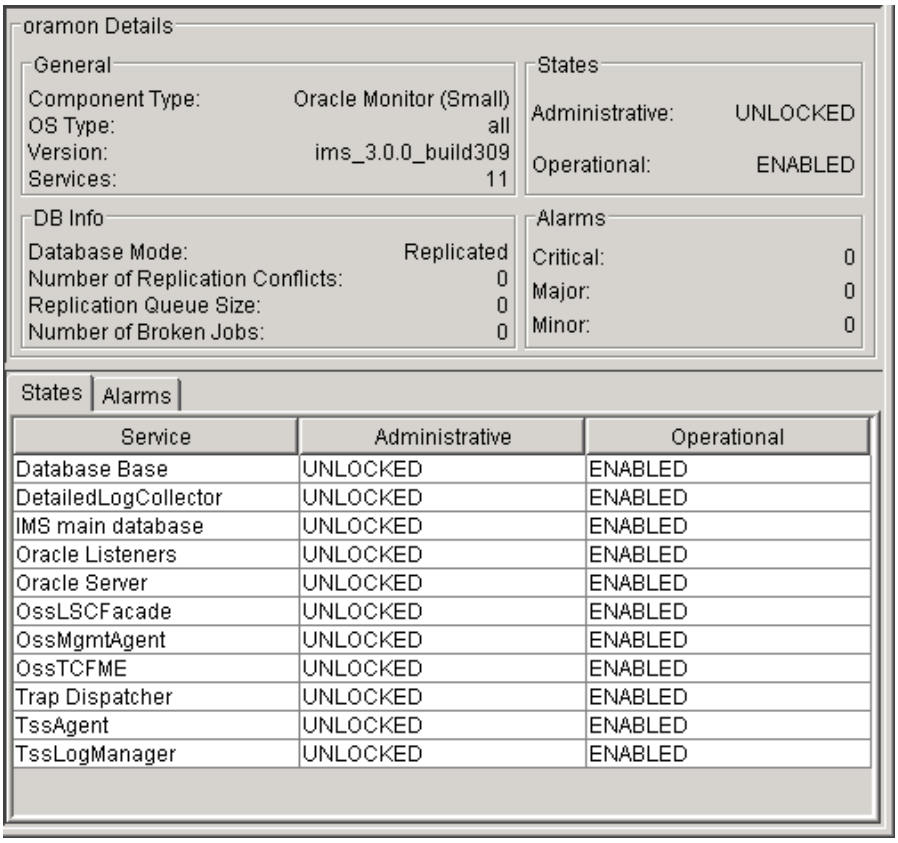
The Oracle Monitor component does not monitor the Oracle database in real time. For details about viewing and responding to alarms in real time, please refer to *CVoIP System Management Console User Guide*.

Information regarding the Oracle Monitor component appears in the General Information Area (GIA) pane when the root level of the Oracle Monitor component is selected within the System Management

Console. Refer to Figure 8, Oracle Monitor: General Information Area (GIA) pane, on page 34.

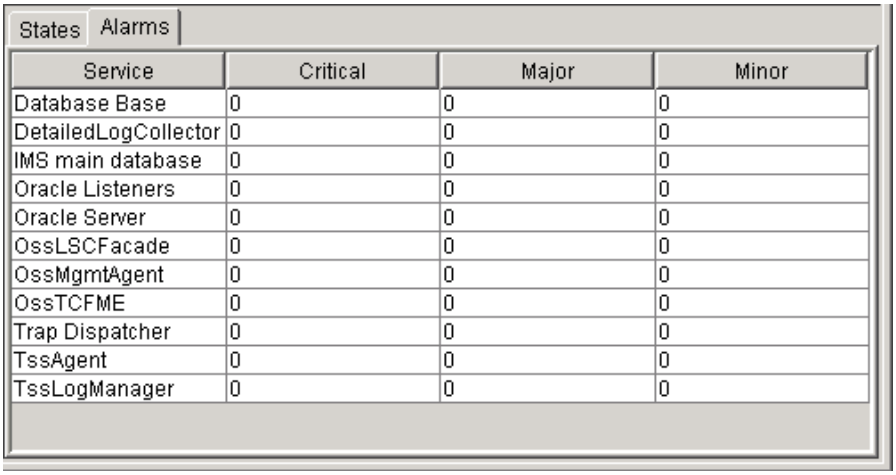
Note: The name of the Oracle Monitor component is customer configurable and may appear differently in your configuration.

Figure 8 Oracle Monitor: General Information Area (GIA) pane



The **Alarms** tab shown in Figure 9, Oracle Monitor: GIA Alarms tab pane, on page 35 lists the number of Critical, Major, and Minor alarms raised by each of the Oracle Monitor services.

Figure 9 Oracle Monitor: GIA Alarms tab pane



Oracle Enterprise Manager Console Monitoring

To launch the OEM Console, please refer to Logging in to the OEM Console on page 73.

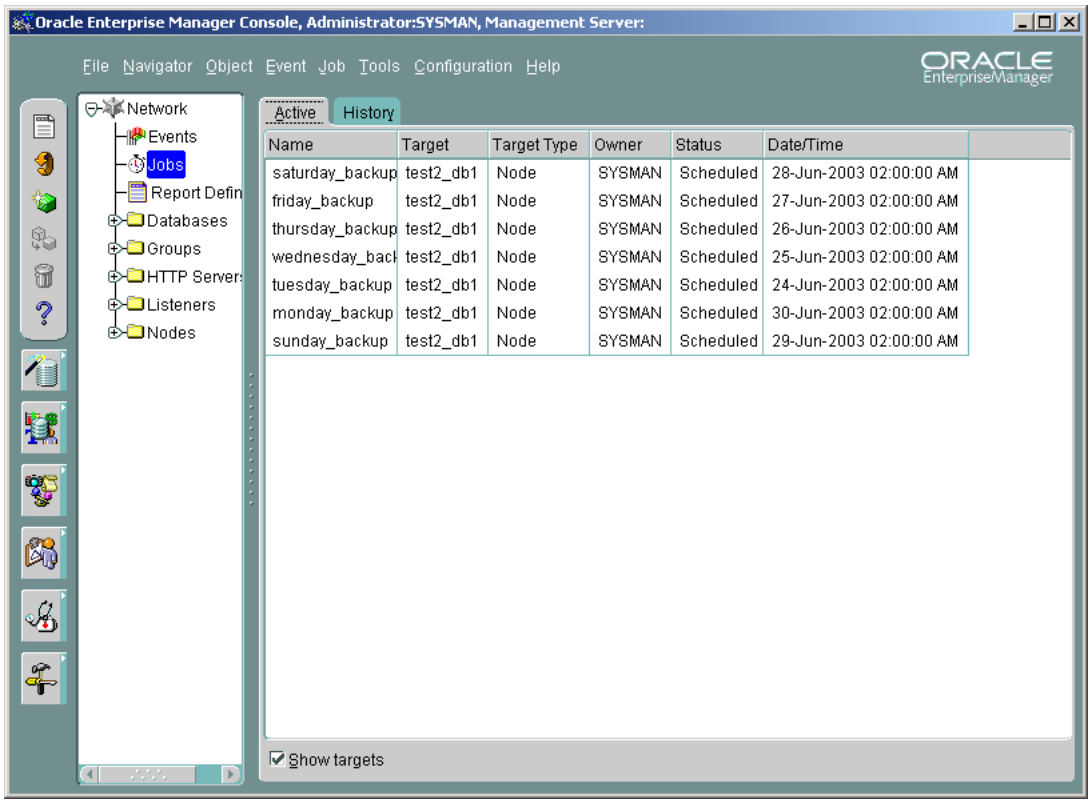
Monitoring database backup jobs

The OEM Console provides status information for all scheduled, database backup jobs. For information on scheduling a database backup job, please refer to Oracle database backups using Export/Import on page 109.

Use the following procedure to view the status and output for database backup jobs:

From the OEM Console

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



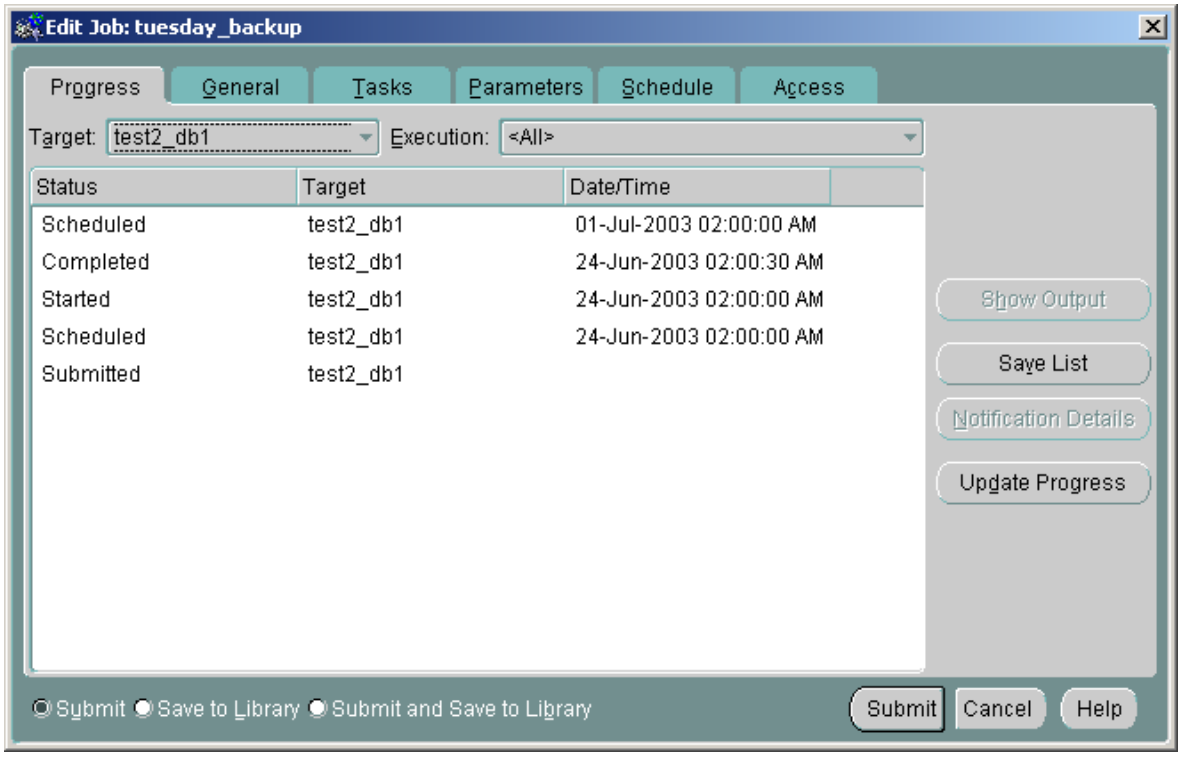
The **Jobs > Active** pane displays the list of active backup jobs that have been scheduled.

2 Select the **History** tab.

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

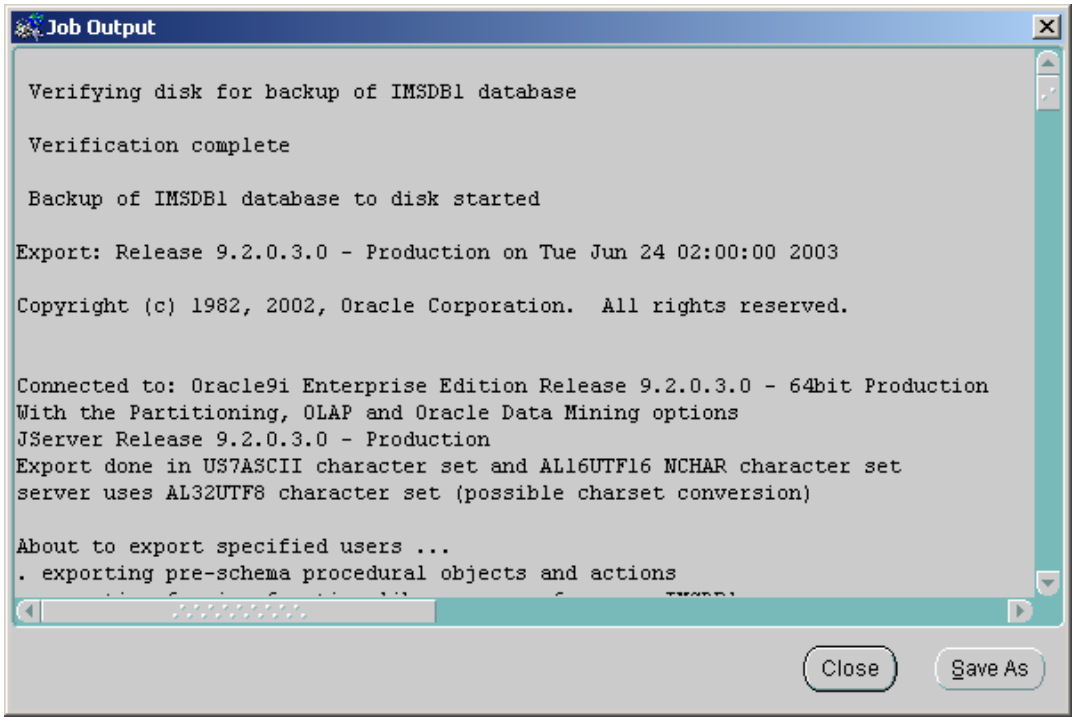
3 In the **History** pane, double-click the appropriate job to display its properties.

The **Edit Job > Progress** window opens, showing when the job was scheduled, 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 information about the job, including the status.



Monitoring alerts

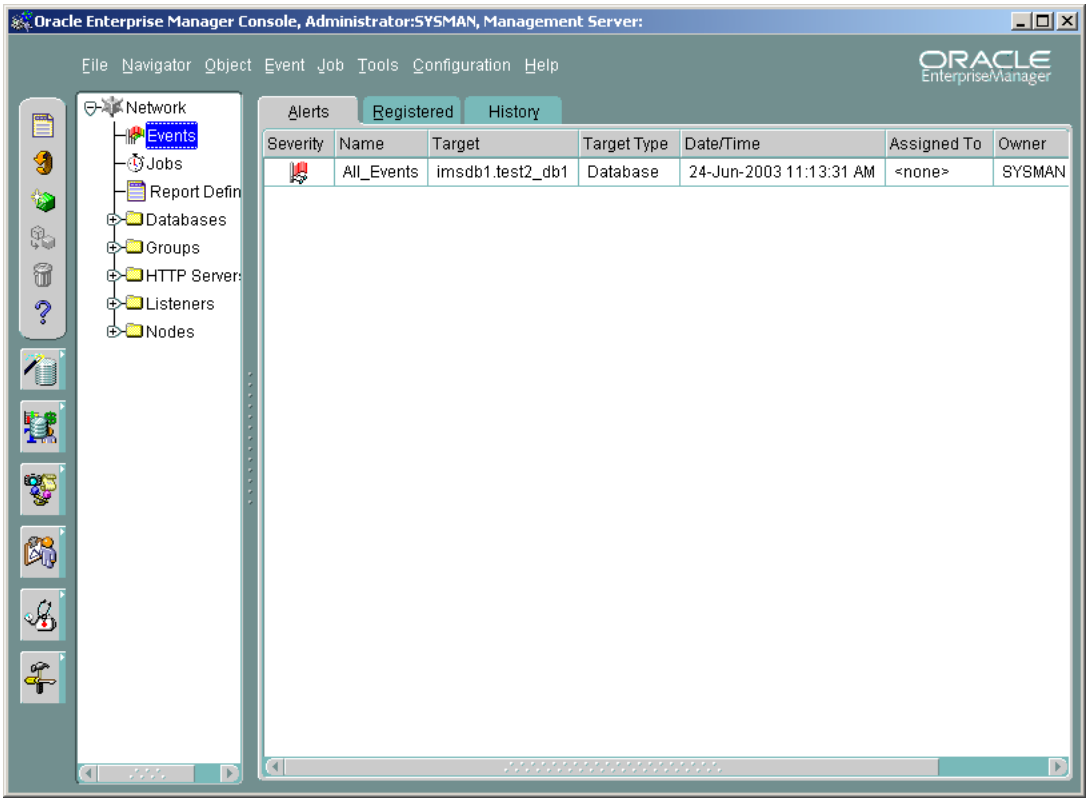
The OEM Console provides a listing of all the current alerts for any registered events.

Use the following procedure to view the current alerts and a history of cleared alerts:

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 events.

3 Click the **History** tab to list all cleared alerts.

Monitoring tablespace usage

Database administrators should regularly monitor tablespaces to ensure that they do not run out of disk space.

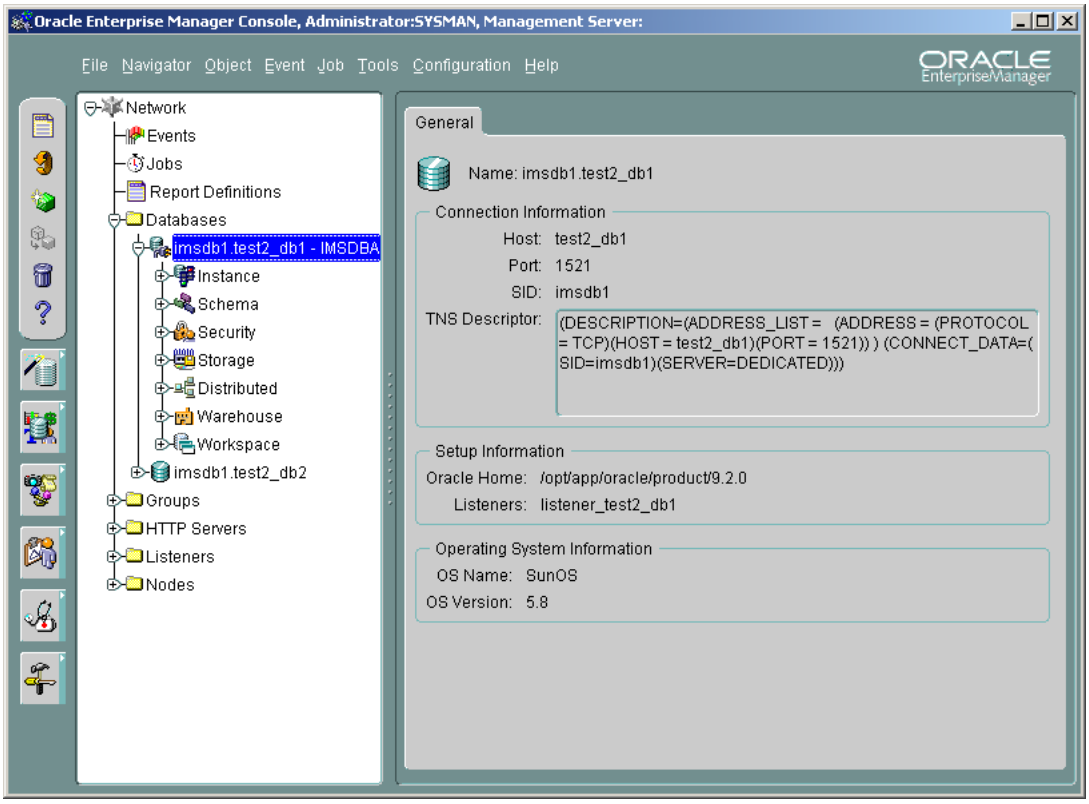
Use the following procedure to view the disk usage for the tablespaces:

From the OEM Console

1 Log in to the OEM Console as **oracle**.

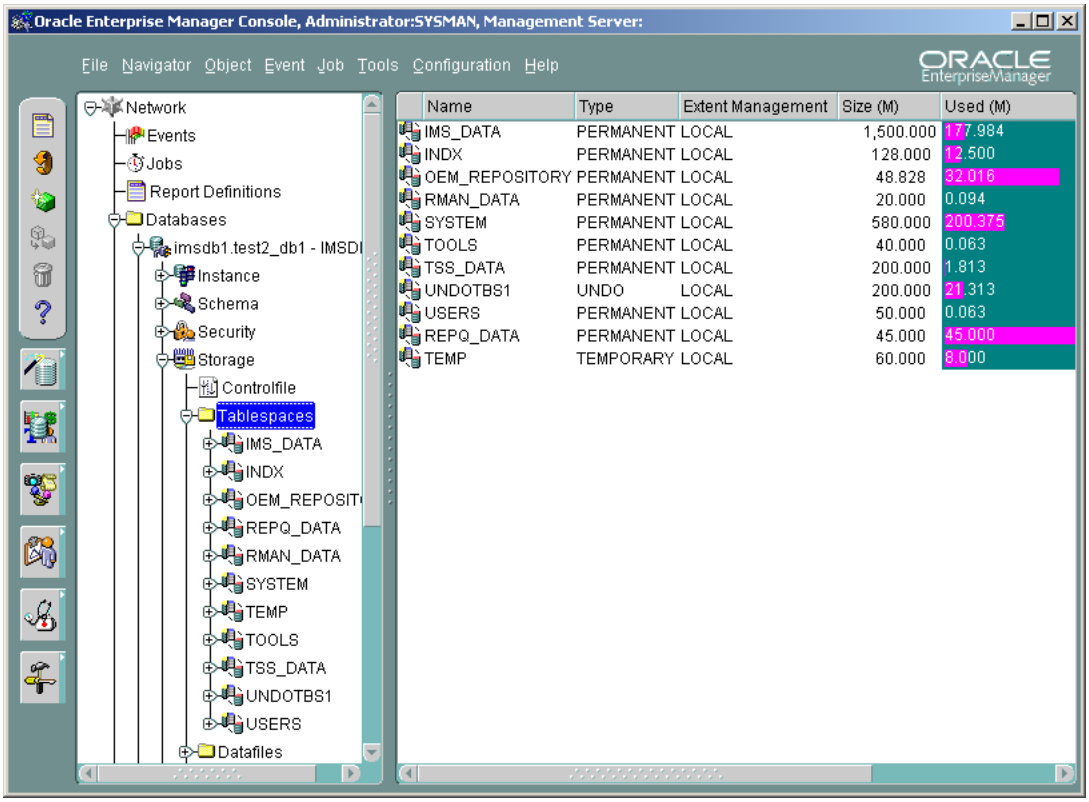
2 From the **Network** tree, select the **Databases** folder and expand the tree.

3 From the **Databases** tree, select the database you want to monitor and expand the tree.



4 Select the **Storage** node and expand it.

5 Select the **Tablespaces** folder and expand it.



A list of tablespaces and data files present in the system displays.

6 Select each tablespace to determine its size, where it is stored, and how much space is available.

7 In the unlikely event that a tablespace should approach its size limits or become full, respond as follows:

If	Do
The tablespace which is approaching its size limits is the UNDOTBS1 (Undo tablespace)	Perform the procedure outlined in Resizing the Undo tablespace on page 48
Any other tablespaces are approaching their size limits	Contact your next level of support for immediate assistance.

Monitoring replication (only in redundant architecture)

Oracle replication should be monitored regularly for replication conflicts between the databases (primary and secondary). The OEM Console provides the status of the replication process between the two databases.

Use the following procedure to monitor the replication status between the two databases:

From the OEM Console

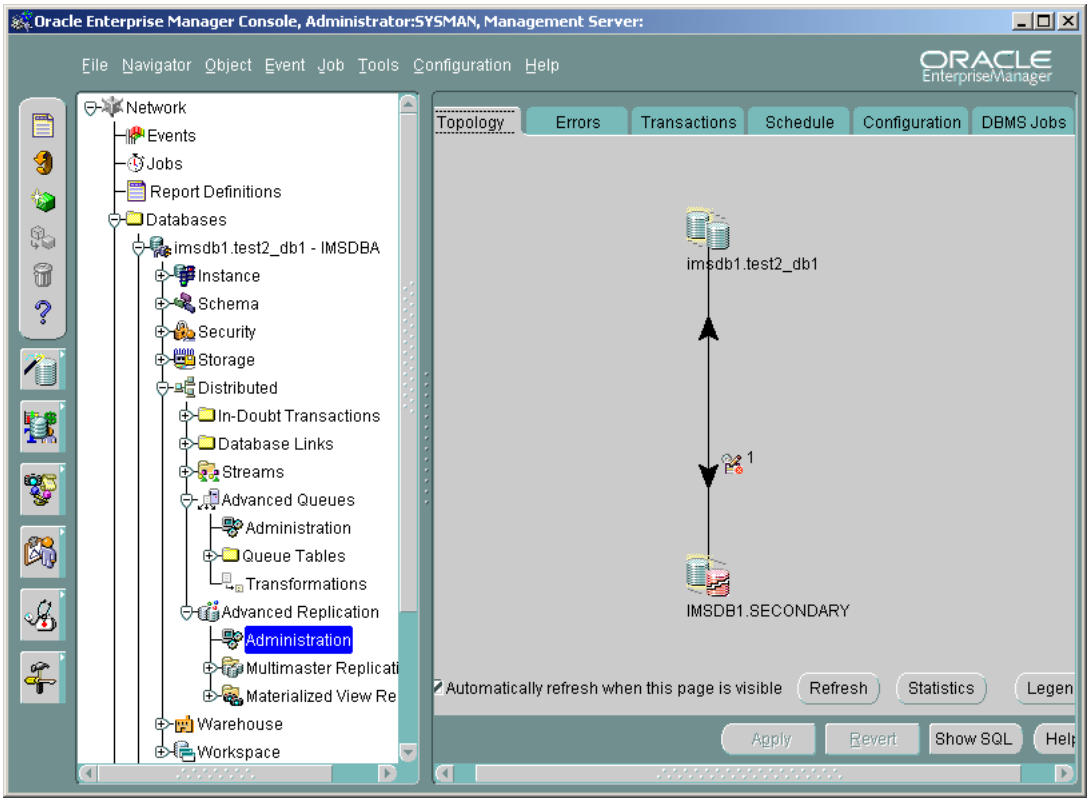
1 Log in as **sysman**.

2 From the **Network** tree, select the **Databases** folder and expand the tree.

3 From the **Databases** tree, select the database you want to monitor and expand the tree.

4 Select **Distributed > Advanced Replication > Administration**.

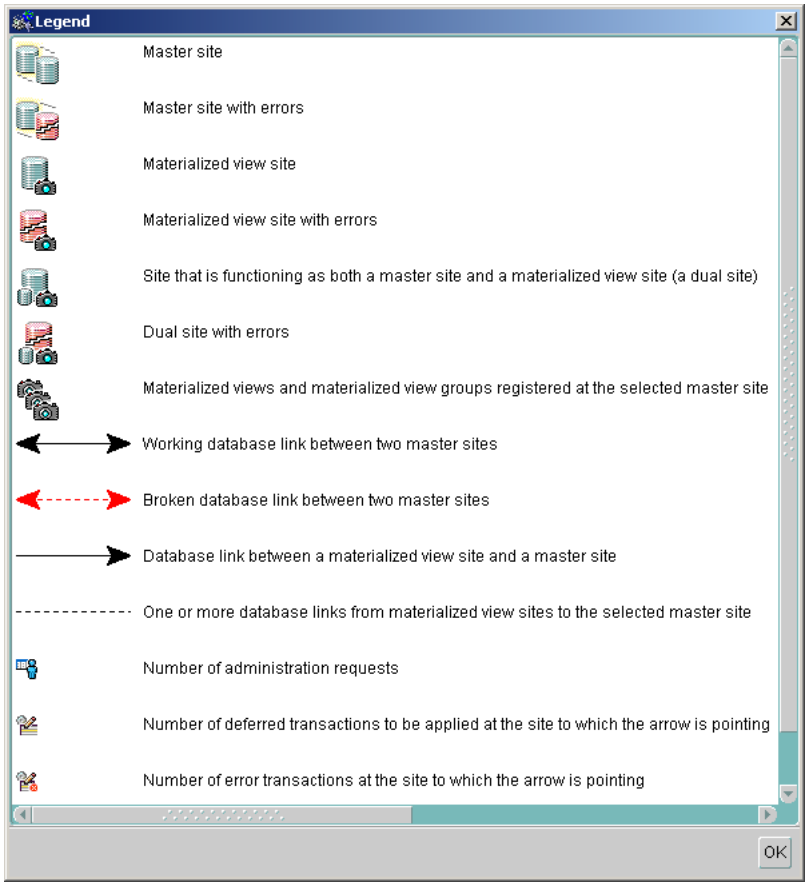
The OEM Console **Administration > Topology** pane opens, displaying the two databases set up in replication mode.



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

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

The **Legend** window opens.



Resolving data transaction errors (only in a redundant architecture)

During replication, data transaction errors (conflicts) may result from the lack of available disk space or errors in the application of queued transactions. If a data transaction error occurs, then a Critical alarm is generated by the Oracle Monitor component of the System Management Console.

ATTENTION

It is also recommended that database administrators monitor error transactions once every 12 hours from the OEM Console.

Use the following procedure to resolve the conflicts from a data transaction error:

From the OEM Console

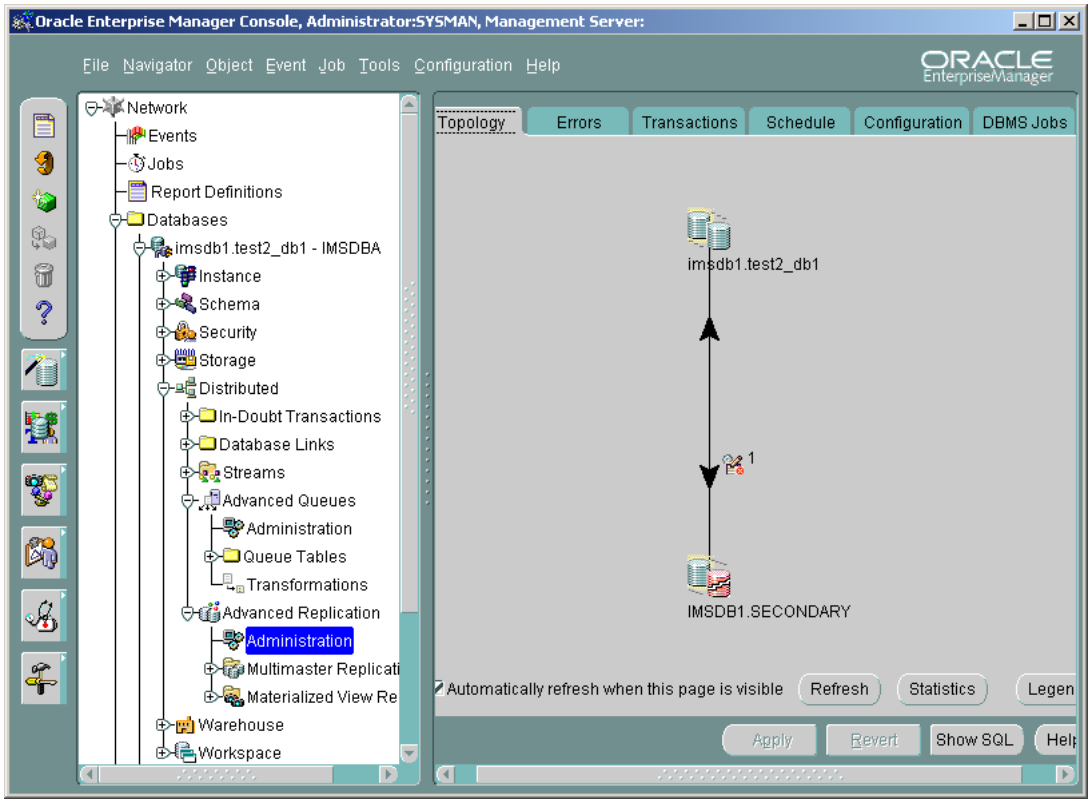
1 Log in as **sysman**.

2 From the **Network** tree, select the **Databases** folder and expand the tree.

3 From the **Databases** tree, select the database you want to monitor and expand the tree.

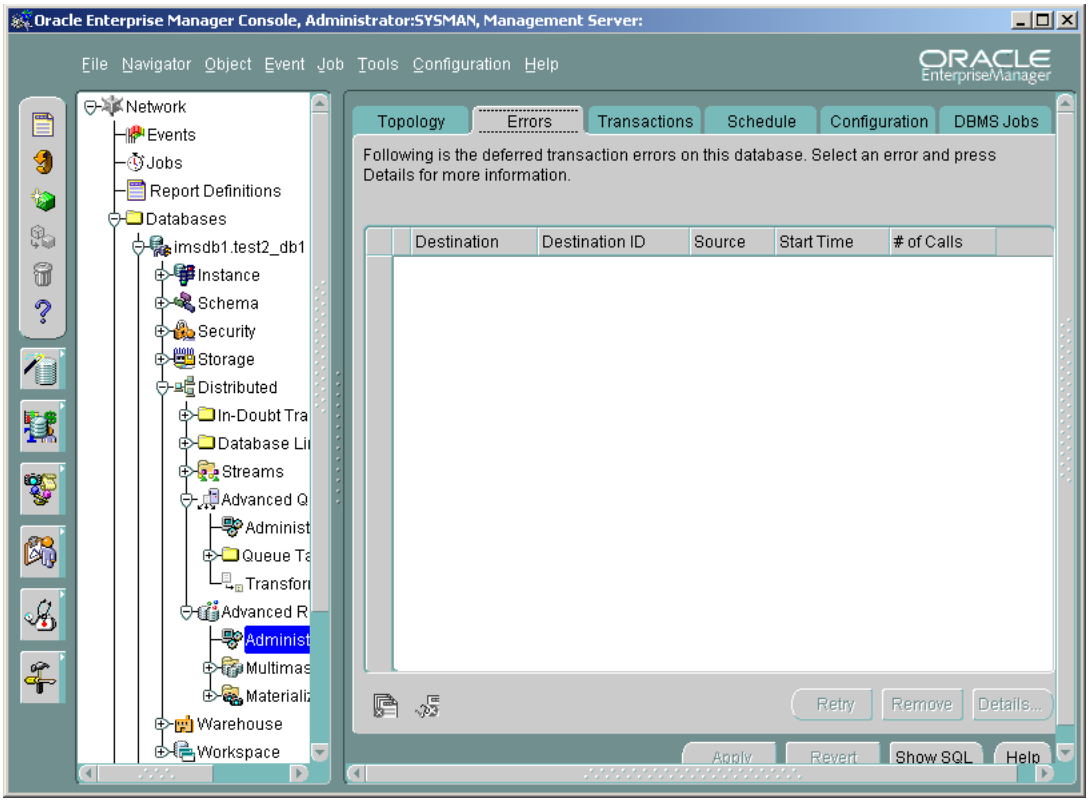
4 Select **Distributed > Advanced Replication > Administration**.

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



5 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.



6 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.

Monitor replication jobs (only in redundant architecture)

Two replication jobs, Push and Purge, are scheduled at initial deployment of the Database Module component. If either of these jobs fail, then a Critical alarm is generated by the Oracle Monitor component

on the System Management Console. In addition, the status of each job can be displayed on the OEM Console.

CAUTION

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

Use the following procedure to monitor and reschedule replication jobs on the OEM console:

From the OEM console

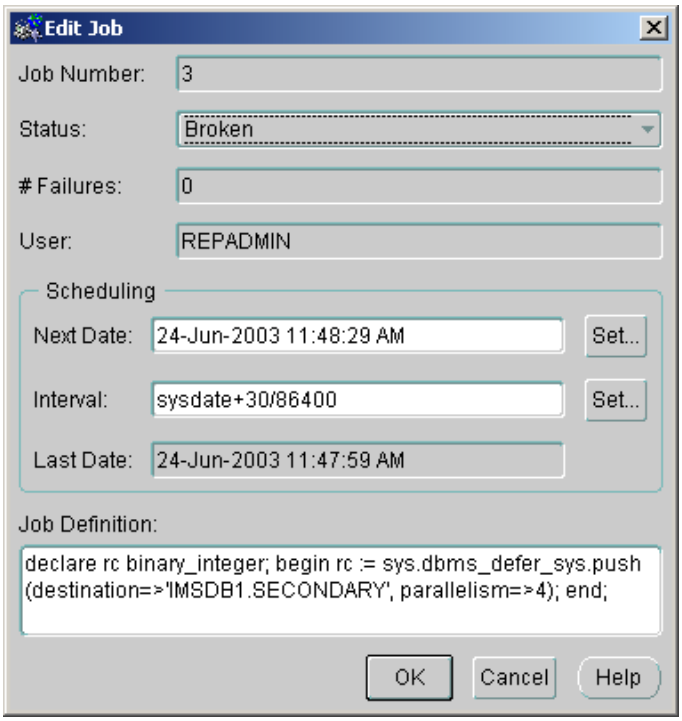
1. Log in to the primary database as **imsdba**.
2. Expand the tree to view **Distributed > Advanced Replication > Administration**.
3. Select the **DBMS Jobs** tab.

   The Push and Purge jobs, along with their status information, displays here. These jobs can be identified by referring to the **Definition** column shown within the **DBMS Jobs** tab.

4 If either of the jobs are broken for any reason, you can reschedule it as follows:

a Select the job and click **Edit**.

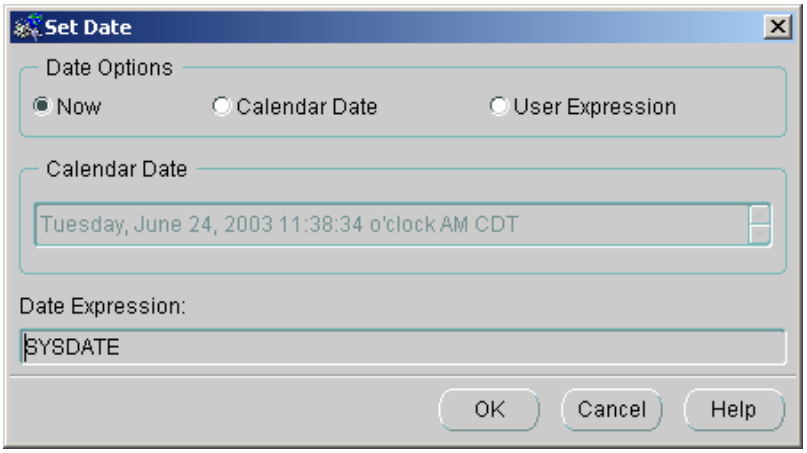
The **Edit Job** window opens.



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**.

Server Monitoring

Monitoring alert log files and trace files

Other database status information is stored in an alert log file. If an alert is produced due to an error, more detailed information regarding the error is placed in the trace file.

Use the following procedure to view details in the alert log files and trace files:

> **ATTENTION**
> It is recommended that database administrators monitor the alert log files and trace files periodically to ensure there are no errors occurring in the Oracle database(s).

In a telnet window

1. Log in as **oracle** to the server hosting the primary or secondary database where the alert 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 logs or errors at the end of the file.

Resizing the Undo tablespace

In cases where a Critical alarm is raised at the System Management Console regarding the exceeding of the disk threshold for the /IMS partition on the server hosting the primary database (or secondary database, in a redundant architecture), it is recommended that the tablespaces sizes/usage be examined via the OEM console. For information on how to perform this monitoring, please refer to Monitoring tablespace usage on page 40.

In the event that the Undo tablespace is reaching its size limit, use the following procedure to resize it:

ATTENTION
Although the following procedure is not service affecting, it is recommended that it only be performed during off-peak hours.

In a telnet window

1 Log in as **oracle** to the server hosting the primary database (or secondary database, when within a redundant architecture) where the alarm has been reported.

2 Execute the following commands:

cd /IMS/imssipdb/data/db_schema/util

./recreateundo.sh <db_type>

where **db_type** is Primary (or Secondary)

Resynchronization (only in a redundant architecture)

In a redundant architecture, the Oracle databases operate in replicated mode, wherein MCS network components 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.

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

CAUTION

Part of the resynchronization process involves placing the databases in the quiesced state (i.e. making both databases read-only).

Only trained personnel should perform the following task.

Resynchronizing (from primary to secondary)

The following procedure should be used when the secondary database must be synchronized with the data from the primary database. In this way, the secondary database is updated with the most current data

which is resident in the primary database. This procedure requires approximately 90 minutes.

Drop replication:

1 Log in as **oracle** to the server hosting the primary database.

2 Execute the following commands:

cd /IMS/imssipdb/data/db_schema/util

remove_replication.sh

Deploy the database bundle to the secondary database server:

3 Log in as **nortel** to the server hosting the mgmtsvr application.

4 Deploy the database software to the server hosting the secondary database by typing the following commands:

dbdeploy.pl

When the script asks for replication, enter N. When the script ask for the type of deployment, choose Install Files only. When the script asks for the pirmary database IP address, enter the IP address of the secondary database server.

Prepare to replicate the database:

5 Log in as **oracle** to the server hosting the primary database.

6 Execute the following commands:

cd /IMS/imssipdb/data/db_schema/logs

pwd (verify that path displayed is the same as path listed in above **cd** command)

rm *

cd /IMS/imssipdb/data/db_schema/util

./prepare_replication.sh

when prompted to restart the database, type **Y**.

Execute the add_secondary_db.sh script:

7 Log in as **oracle** to the server hosting the primary database.

8 Execute the following commands:

cd /IMS/imssipdb/data/db_schema/util

./add_secondary_db.sh

This command performs a backup of the primary database. This also copies the data up to a given SCN and starts the queuing

of all changes made to the primary database. This step requires approximately 20 minutes.

Setup replication:

9 Log in as **oracle** to the server hosting the secondary database.

10 Execute the following commands:

cd /IMS/imssipdb/data/db_schema/util

./activate_secondary_db.sh <primary_DB_hostname>

Note: The activate_secondary_db.sh script uses Secure FTP to transfer the backup (taken above) from the primary database to the secondary database. If this is the first time Secure FTP has been used on this server, the administrator will be prompted to confirm the authenticity of the host with the following question: The authenticity of host ... can't be established. RSA key fingerprint ... Are you sure you want to continue connecting (yes/no)? Type **yes** in response.

when prompted for the "oracle@<hostname> password", enter the oracle password for the primary database

when prompted to restart the database, type **Y**.

This step requires approximately 40 minutes.

Turn off archiving logs on primary database:

11 Log in as **oracle** to the server hosting the primary database.

12 Execute the following commands:

cd /export/home/oracle/bin

./archivallogctl off

when prompted to restart the database, type **Y**.

Clean up the primary and secondary databases:

13 Log in as **oracle** to the server hosting the primary database.

14 Execute the following commands:

cd /IMS/imssipdb/data/db_schema/util

./clean.sh

15 Repeat this procedure on the server hosting the secondary database.

Re-configure the database SNMP agent:

16 Log in as **root** to the server hosting the secondary database.

17 Execute the following commands:

cd /export/home/oracle/bin

./config_snmp

This step is necessary because the replication process overwrites the password of the DBMCPSNMP account on the secondary database server.

Undeploy the database bundle from the secondary database server:

18 Log in as **nortel** to the secondary database server.

19 Undeploy the software by typing the following commands:

dsmundeploy -load <dbload> -node <secondary_db_ip>

Resynchronization (from secondary to primary)

Use this procedure to synchronize both databases to the data in the secondary database. This might be necessary if the server hosting the primary database experienced a hardware failure and was replaced with a new server. In this way, the primary database is updated with the most current data which is resident in the secondary database. This procedure requires approximately 90 minutes.

Drop replication:

1 Log in as **oracle** to the server hosting the primary database.

2 Execute the following commands:

cd /IMS/imssipdb/data/db_schema/util

remove_replication.sh

Deploy the database bundle to the secondary database server:

3 Log in as **nortel** to the server hosting the mgmtsvr application.

4 Deploy the database software to the server hosting the secondary database by typing the following commands:

dbdeploy.pl

When the script asks for replication, enter N. When the script ask for the type of deployment, choose Install Files only. When the script asks for the pirmary database IP address, enter the IP address of the secondary database server.

Prepare to replicate the database:

5 Log in as **oracle** to the server hosting the secondary database.

6 Execute the following commands:

cd /IMS/imssipdb/data/db_schema/logs

pwd (verify that path displayed is the same as path listed in above **cd** command)

rm *

cd /IMS/imssipdb/data/db_schema/util

./prepare_replication_at_secondary.sh

when prompted to restart the database, type **Y**.

Execute the add_primary_db.sh script:

7 Log in as **oracle** to the server hosting the secondary database.

8 Execute the following commands:

cd /IMS/imssipdb/data/db_schema/util

./add_primary_db.sh

This command performs a backup of the secondary database. This also copies the data up to a given SCN and starts the queuing of all changes made to the secondary database. This step requires approximately 20 minutes.

Setup replication:

9 Log in as **oracle** to the server hosting the primary database.

10 Execute the following commands:

cd /IMS/imssipdb/data/db_schema/util

./activate_primary_db.sh <secondary_DB_hostname>

Note: The activate_primary_db.sh script uses Secure FTP to transfer the backup (taken above) from the secondary database to the primary database. If this is the first time Secure FTP has been used on this server, the administrator will be prompted to confirm the authenticity of the host with the following question: The authenticity of host ... can't be established. RSA key fingerprint ... Are you sure you want to continue connecting (yes/no)? Type **yes** in response.

when prompted for the "oracle@<hostname> password", enter the oracle password for the secondary database

when prompted to restart the database, type **Y**.

This step requires approximately 40 minutes.

Turn off archiving logs on secondary database:

11 Log in as **oracle** to the server hosting the secondary database.

12 Execute the following commands:

cd /export/home/oracle/bin

./archivallogctl off

when prompted to restart the database, type **Y**.

Clean up the primary and secondary databases:

13 Log in as **oracle** to the server hosting the primary database.

14 Execute the following commands:

cd /IMS/imssipdb/data/db_schema/util

./clean.sh

15 Repeat this procedure on the server hosting the secondary database.

Re-configure the database SNMP agent:

16 Log in as **root** to the server hosting the primary database.

17 Execute the following commands:

cd /export/home/oracle/bin

./config_snmp

This step is necessary because the replication process overwrites the password of the DBMCPSNMP account on the primary database server.

Undeploy the database bundle from the secondary database server:

18 Log in as **nortel** to the secondary database server.

19 Undeploy the software by typing the following commands:

dsmundeploy -load <dbload> -node <secondary_db_ip>

Database and Oracle Monitor alarm descriptions

Once in operation, system elements have the ability to raise and clear alarms/faults. As faults occur, alarms are generated by the element and sent to the Management Module component. Once at the Management Module, administrators can view the alarms using the System Management Console's alarm browser.

When an alarm is raised, it is added to a list of active alarms. The alarm remains on the active list until it is resolved. Once the problem is resolved, the alarm is cleared and removed from the list of active alarms.

Every alarm generates an associated log. Administrators view alarm information in log format using the log browser. The format of an alarm, viewed from the log browser, is different from the format that is displayed through the alarm browser.

For more background information on alarms and logs, refer to *CVoIP Management Module Basics*. For information on using the alarm and log browsers, refer to *CVoIP System Management Console User Guide*.

The following table lists the alarms specific to the database and viewed in the System Management Console. Click on the link to view the component's alarm descriptions.

Table 6 Alarm families of the Database and Oracle Monitor components

Short name	Long name*	Component or services generating alarm
DBF	DFB-OAM	DatabaseFactory DBF (DatabaseFactory) alarm descriptions
ODB	ORCL-DB	Oracle Database ODB (Oracle Monitor alarms about the Database) alarm descriptions
ORCL	ORCL	Oracle ORCL (Oracle Database) alarm descriptions
* The long name is used in the FamilyName column of the alarm browser.		

DBF (DatabaseFactory) alarm descriptions

DBF alarms are raised by the DatabaseFactory service of applications with connections to the database(s).

Table 7 DBF101

Alarm Name:	Primary DB Not Connected
Alarm ID:	DBF101
Category:	COMMUNICATIONS
Severity:	Minor
Description:	The application is not connected to the primary database.
Corrective Action:	Check the primary database. The alarm clears when connectivity to the database is restored.

Table 8 DBF102

Alarm Name:	Secondary DB Not Connected
Alarm ID:	DBF102
Category:	COMMUNICATIONS
Severity:	Minor
Description:	The application is not connected to the secondary database.
Corrective Action:	Check the secondary database. The alarm clears when connectivity to the secondary database is restored.

Table 9 DBF103

Alarm Name:	No Database Available
Alarm ID:	DBF103
Category:	COMMUNICATIONS
Severity:	Critical
Description:	The application is unable to connect to any database. Primary Database is <primary db ip address>: Secondary Database is <secondary db ip address>.
Corrective Action:	Check the database servers. The alarm is cleared when connectivity to a database is restored.

ODB (Oracle Monitor alarms about the Database) alarm descriptions

Oracle Monitor alarms monitor the status of the database.

Table 10 ODB701

Alarm Name:	Oracle Server Operation Alarm
Alarm ID:	ODB701
Category:	PROCESSING_ERROR
Severity:	Critical
Description:	Failed to initialize.
Corrective Action:	Ensure SNMP configuration data is valid and SNMP agent is running. If the problem persists, contact your next level of support.

Table 11 ODB702

Alarm Name:	Oracle Listener Alarm
Alarm ID:	ODB702
Category:	PROCESSING_ERROR
Severity:	Minor
Description:	No Oracle listeners were found.
Corrective Action:	Ensure SNMP configuration data is valid. If the problem persists, contact your next level of support.

Table 12 ODB703

Alarm Name:	Oracle Listener Timeout Alarm
Alarm ID:	ODB703
Category:	PROCESSING_ERROR
Severity:	Critical
Description:	Failed to initialize. SNMP query made to OID: 1.3.6.1.2.1.27.1.1.2 searching for index of configured value: Oracle Server = imsdb1Using configured values port: 9161 and IP address: <ip address> Timed out waiting for SNMP response.
Corrective Action:	Ensure SNMP configuration data is valid and SNMP agent is running. If the problem persists, contact your next level of support.

Table 13 ODB704

Alarm Name:	Database Unavailable Alarm
Alarm ID:	ODB704
Category:	PROCESSING_ERROR
Severity:	Critical
Description:	Database is not available.
Corrective Action:	Ensure both database and SNMP agent are running. Restart the database if needed.

Table 14 ODB705

Alarm Name:	Database Unknown State Alarm
Alarm ID:	ODB705
Category:	PROCESSING_ERROR
Severity:	Minor
Description:	Database is in an UNKNOWN state.
Corrective Action:	Ensure both database and SNMP agent are running. Restart the SNMP agent if needed.

Table 15 ODB706

Alarm Name:	Database Operation Status Alarm
Alarm ID:	ODB706
Category:	PROCESSING_ERROR
Severity:	Critical
Description:	Database is in UNAVAILABLE state.
Corrective Action:	Ensure both database and SNMP agent are running. Restart the SNMP agent if needed.

Table 16 ODB707

Alarm Name:	Oracle Server Down
Alarm ID:	ODB707
Category:	PROCESSING_ERROR
Severity:	Critical
Description:	Detected Oracle Server operational state to be DOWN.
Corrective Action:	Ensure Oracle server and SNMP agent are running correctly. Restart Oracle server or the snmp agent if needed. If the problem persists, contact your next level of support.

ORCL (Oracle Database) alarm descriptions

Oracle Database (ORCL) alarms report problems with database operations.

Table 17 ORLC701

Alarm Name:	Broken Jobs
Alarm ID:	ORLC701
Category:	PROCESSING_ERROR
Severity:	Critical
Description:	<Number of> broken jobs exist in the database
Corrective Action:	Correct the problem using OEM, or contact your next level of support.

Table 18 ORLC702

Alarm Name:	Replication Conflicts
Alarm ID:	ORLC702
Category:	PROCESSING_ERROR
Severity:	Critical
Description:	Replication conflicts exist in the database.
Corrective Action:	If the conflicts are due to registrations, they can be safely deleted using OEM, otherwise contact your next level of support.

Table 19 ORLC703

Alarm Name:	Replication Queue
Alarm ID:	ORLC703
Category:	PROCESSING_ERROR
Severity:	Critical
Description:	Replication queue size of <size> exceeds maximum threshold value of <maximum queue size>
Corrective Action:	Attempt resolving the problem through OEM, or contact your next level of support.

Configuration management

How this chapter is organized

This chapter is organized as follows:

Functional description

The following deployment tasks related to the Database functionality are performed during installation and commissioning or when upgrading to a full release:

- Addition and configuration of the server(s) hosting the Database functionality.
- Installation of Oracle onto the server(s), including the creation of the **oracle**, **sysman**, and **system** administrator accounts.
- Addition and configuration of the Database Module software component onto the server hosting the primary database.

  Note: In a redundant architecture, the Database Module component is not deployed on the server hosting the secondary database. When an update is made to the Database Module component (located on the server hosting the primary database), the new schema information is communicated to the secondary database.

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

Tools and utilities

Use the following tools for configuring the Database functionality:

- **System Management Console:** Launches the OEM Console and used for deployment and configuration of the Oracle Monitor component(s).
- **Oracle Enterprise Manager (OEM) Console:** Used by the database administrator to setup preferences for the **sysman** administrator and to setup an observer account.

Tasks

Table 1, Configuration management tasks, on page HIDDENTable 20, Configuration management tasks, on page 63 lists the configuration tasks for the Database functionality.

Table 20 Configuration management tasks

Topic	Subtopic	Procedure
System Management Console Configuration Management	Database Base service	Component database connection configuration on page 64
	Oracle Monitor component	Adding the Oracle Monitor component on page 65
	Oracle Monitor component	Querying or modifying Oracle Monitor configuration properties on page 66
Oracle Enterprise Manager Console Configuration Management	Log in	Logging in to the OEM Console on page 73
	sysman preferences	Configuring sysman preferences on page 76
	Read-only user	Configuring a database observer account on page 79
Server Configuration Management	System and General Administrators	Configuring administrator roles on page 83

System Management Console configuration management

Component database connection configuration

The following MCS network components have a service called Database Base where the administrator must configure database IP addresses as part of their configuration.

- Oracle Monitor
- Management Module

For details about configuring MCS network component connections to the Oracle database(s), see the related component documents. Table 21, Component Database Base configuration properties, on page 64 lists the configuration properties used by MCS network components to set up access to the Oracle database(s).

Table 21 Component Database Base 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 MCS network component has to the database ***Note:*** Do not change the Connections value. The number of connections required varies between MCS network components. ***Note:*** This value is not allowed to be changed for the Oracle Monitor component.

Adding the Oracle Monitor component

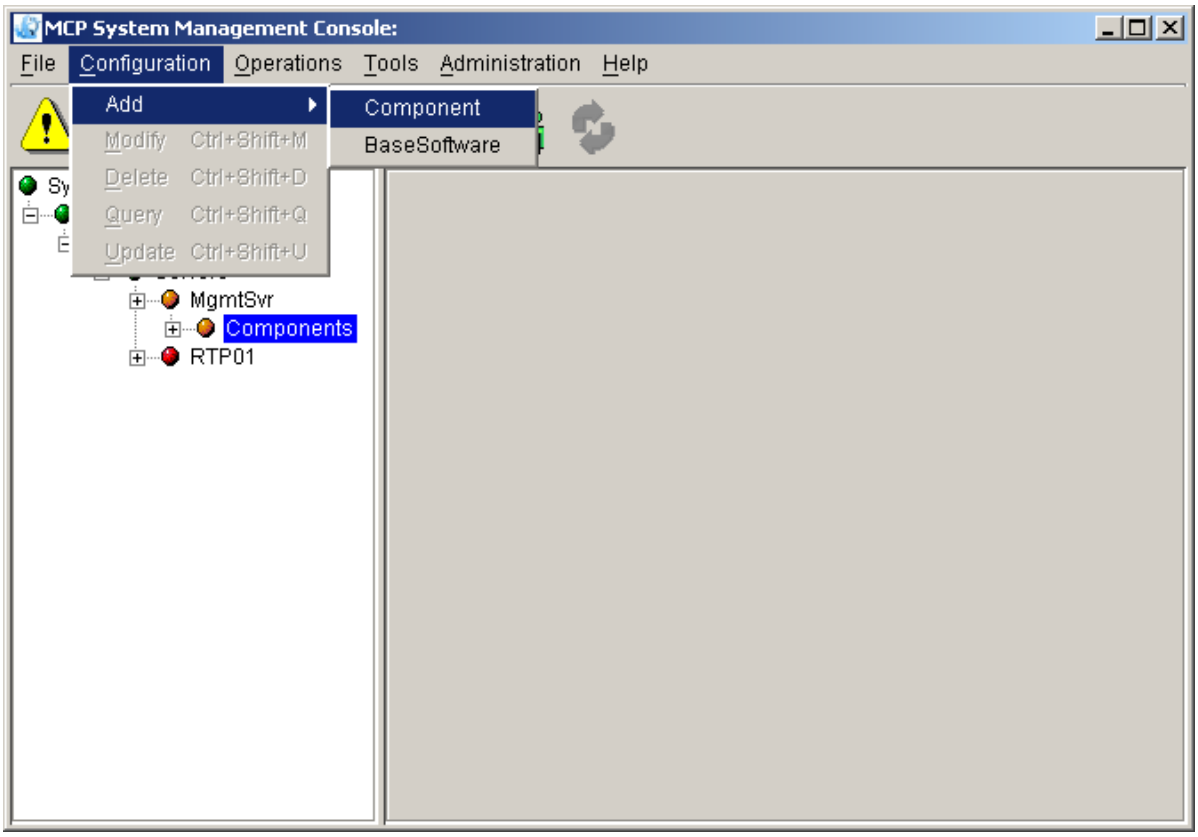
Use the following procedure to add/deploy the Oracle Monitor component:

From the System Management Console

1 In the System tree, select **Components** under the appropriate server hosting a database.

2 From the Configuration menu, select the **Add > Component** command.

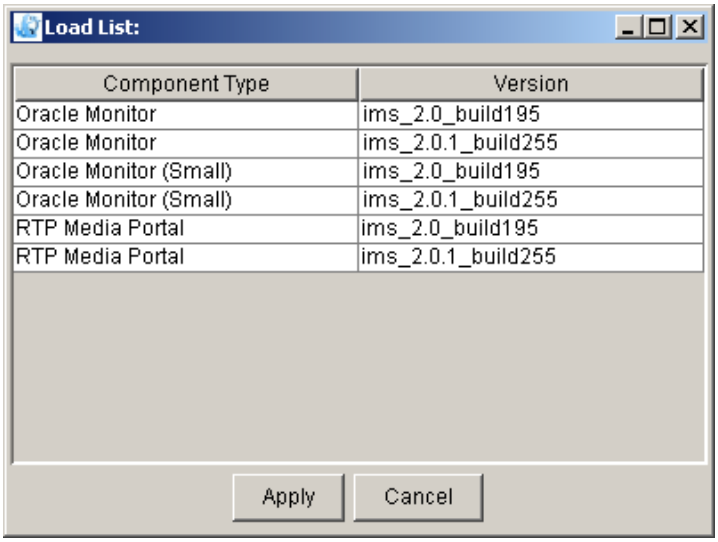
Figure 10 Add from the Configuration menu



You can also launch the update command by right-clicking **Components** and selecting **Add > Component** from the pop-up menu.

3 After **Add > Component** is selected, the Load List window appears with all available MCS network component loads (except for those components already deployed to the server).

Figure 10 Load list for adding



4 Select the desired software load version for the Oracle Monitor component. Click on the **Apply** button.

5 You will be prompted to configure the Oracle Monitor configuration tabs and properties.

Note: It is recommended that all of the default configuration values be used when configuring the Oracle Monitor component. The only exception is the Primary Host field in the Database Base service tab. This field should be filled in with the IP address of the server (as indicated by the server selected in **step 1** above), even when indicating the server hosting the secondary database.

6 After entering the appropriate configuration information, enter a label (six characters or less) in the Service Component Name field. This label is the name that appears in the System tree. Click on the **Apply** button. A progress window appears while it deploys.

7 When deployment completes, a window will appear showing that the component was added successfully.

8 Within a redundant architecture, repeat this procedure on the server hosting the secondary database.

Querying or modifying Oracle Monitor configuration properties

Use the following procedure to query or modify the configuration properties for the Oracle Monitor component:

From the System Management Console

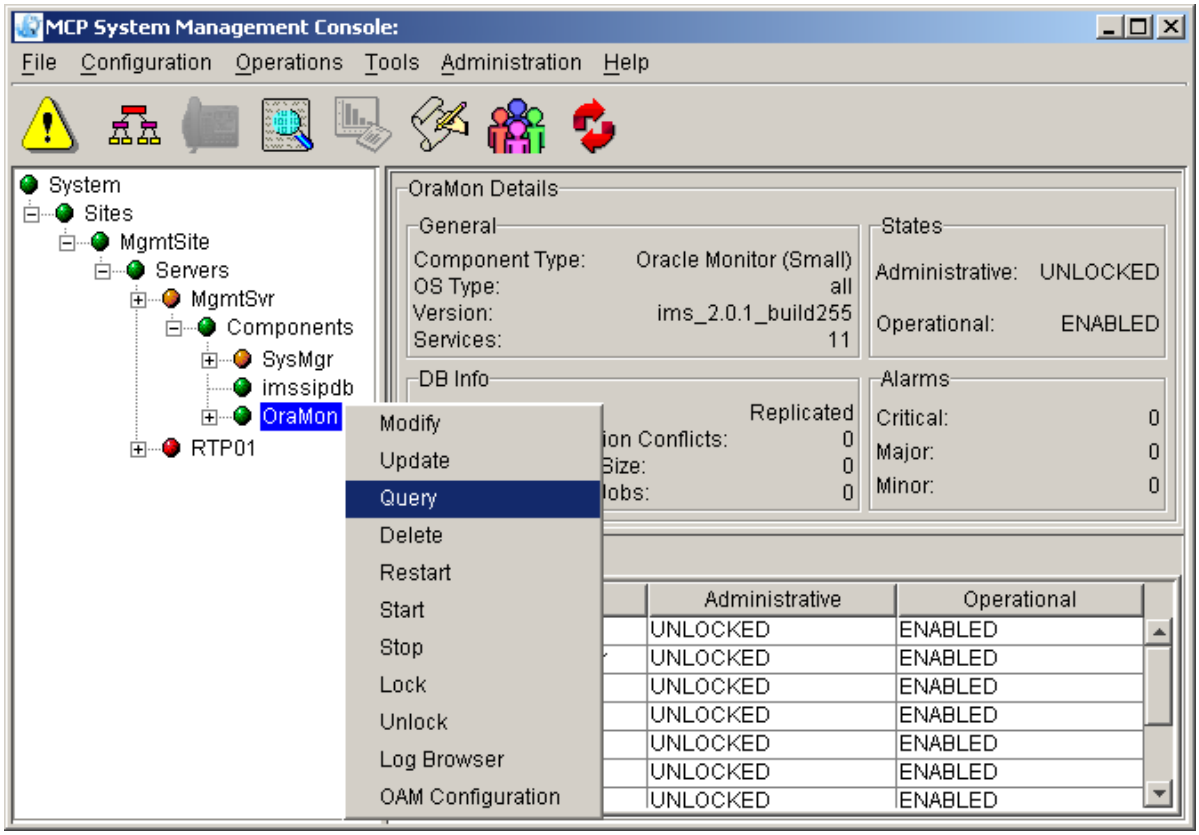
1 In the System tree, find the appropriate Oracle Monitor component to be queried or modified.

Note: In a redundant architecture, there are two Oracle Monitor components deployed (each on separate servers where the primary and secondary database resides).

2 To query the configuration properties of an Oracle Monitor component, select the root level Oracle Monitor component for the primary database or secondary database.

3 From the Configuration menu, select the **Query** command.

Figure 11 Query Oracle Monitor Configuration properties



The Query Oracle Monitor window displays the properties. However, no configuration changes are permitted in the window.

4 To modify the configuration properties of a Oracle Monitor component, do the following:

a Select the root level Oracle Monitor component.

b From the Operations menu, select the **Lock** command.

Note: In order to modify configuration properties, a component must be in the LOCKED state.

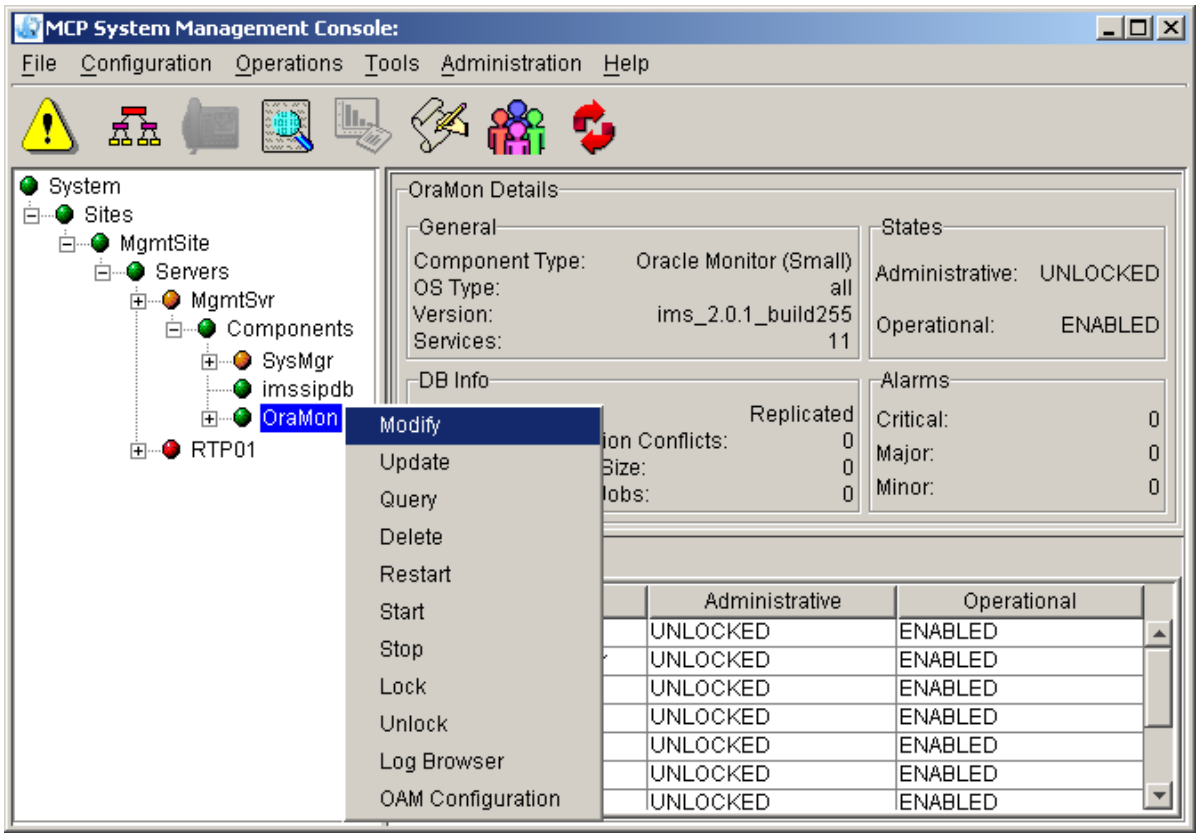
c A confirmation dialog box prompts you to confirm that you want to lock the Oracle Monitor. Click **Yes**.

Note: Locking the Oracle Monitor has no effect on the component being monitored (in this case the primary or secondary database).

d Select the root level Oracle Monitor component.

e From the Configuration menu, select the **Modify** command.

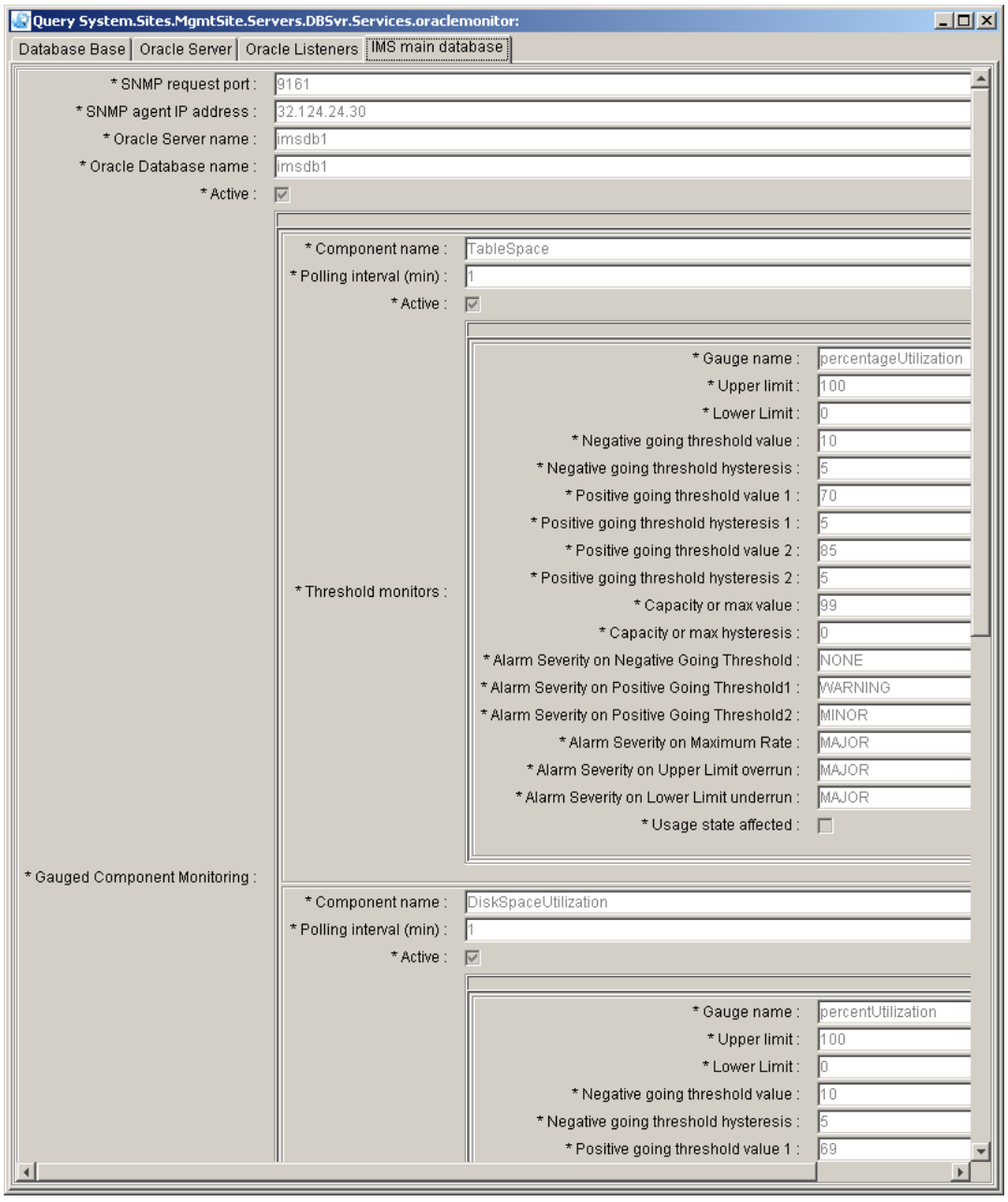
Figure 12 Modify Oracle Monitor Configuration properties

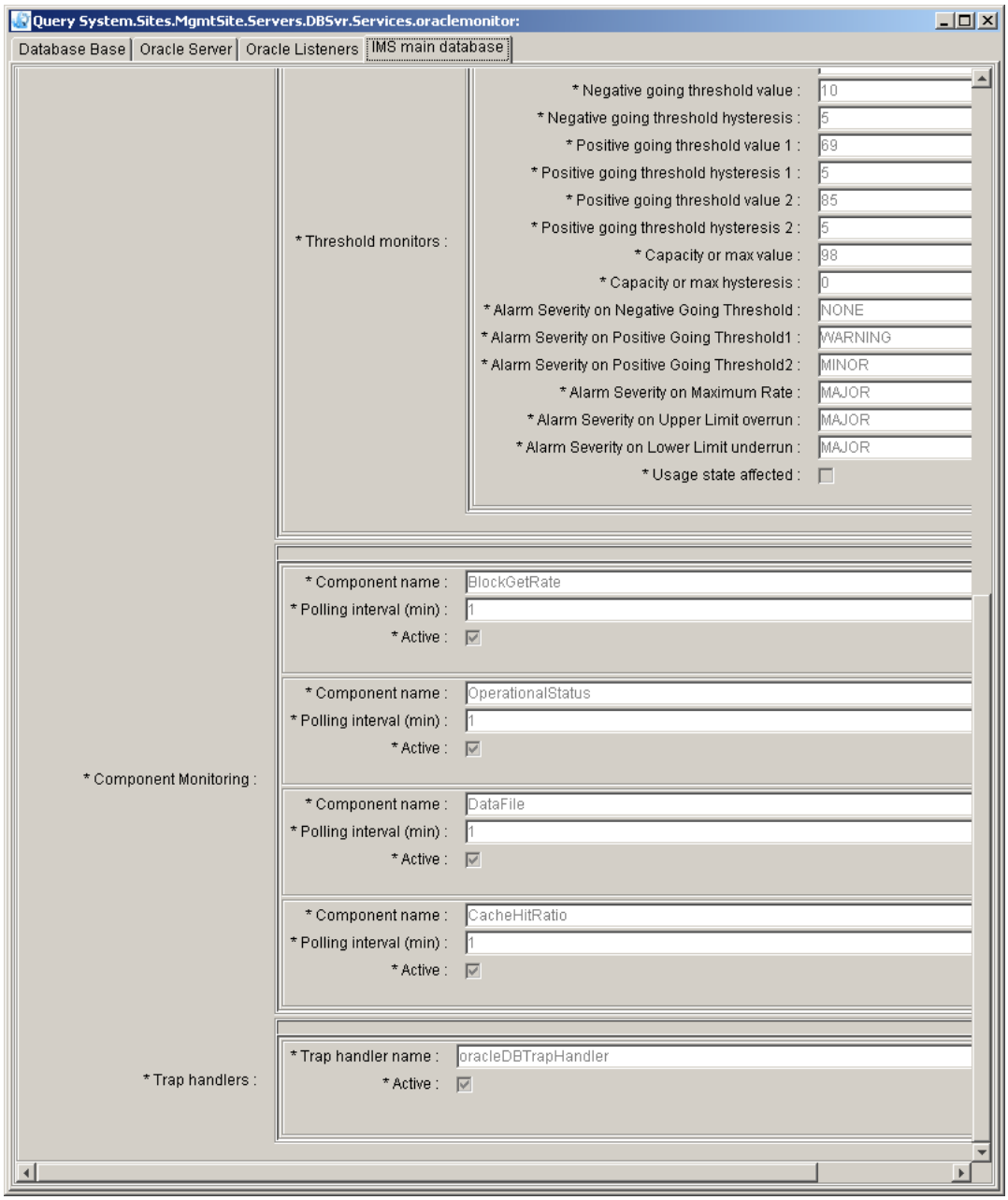


f Modify the properties as required and click **OK**.

IMS Main Database tab

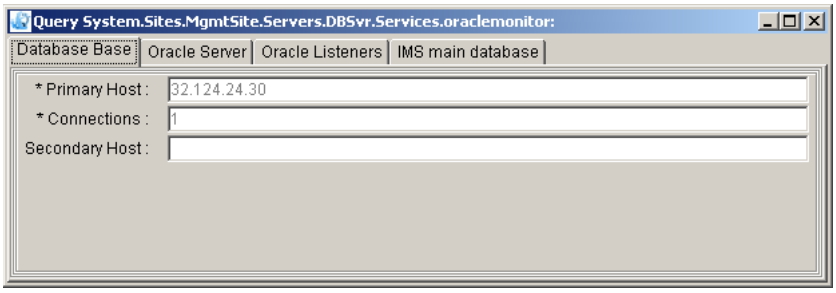
The following figures show the fields available for query or modification from the **IMS Main Database** tab of the **Query** or **Modify Oracle Monitor** dialog box:




Query System.Sites.MgmtSite.Servers.DBSvr.Services.oraclemonitor:
Database Base
Oracle Server
Oracle Listeners
IMS main database
* Threshold monitors :
* Negative going threshold value : 10
* Negative going threshold hysteresis : 5
* Positive going threshold value 1 : 69
* Positive going threshold hysteresis 1 : 5
* Positive going threshold value 2 : 85
* Positive going threshold hysteresis 2 : 5
* Capacity or max value : 98
* 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 :
* Component name : BlockGetRate
* Polling interval (min) : 1
* Active :
* Component name : OperationalStatus
* Polling interval (min) : 1
* Active :
* Component name : DataFile
* Polling interval (min) : 1
* Active :
* Component name : CacheHitRatio
* Polling interval (min) : 1
* Active :
* Trap handlers :
* Trap handler name : oracleDBTrapHandler
* Active :

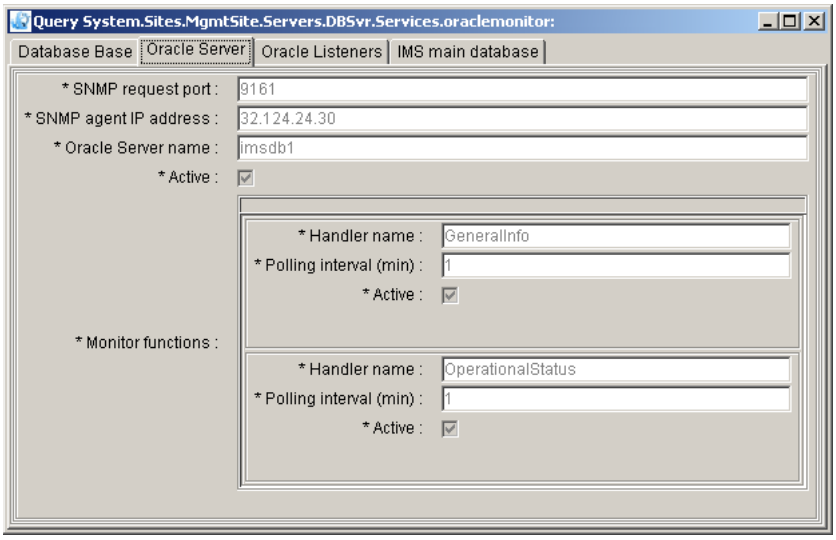
Database Base tab

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:



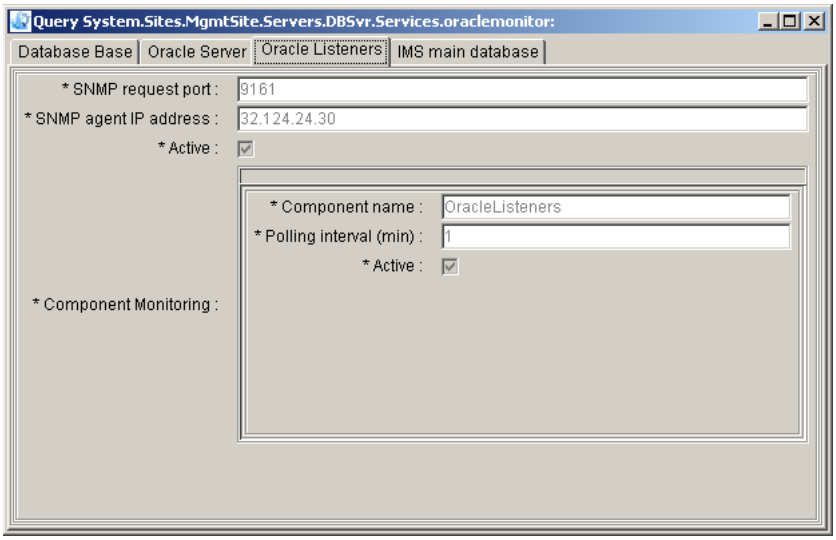
Oracle Server tab

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:



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:


Query System.Sites.MgmtSite.Servers.DBSvr.Services.oraclemonitor:
Database Base
Oracle Server
Oracle Listeners
IMS main database
* SNMP request port :
9161
* SNMP agent IP address :
32.124.24.30
* Active :
* Component name :
OracleListeners
* Polling interval (min) :
1
* Active :
* Component Monitoring :

Oracle Enterprise Manager Console configuration management

Logging in to the OEM Console

Use the following procedure to log in to the OEM Console from the System Management Console:

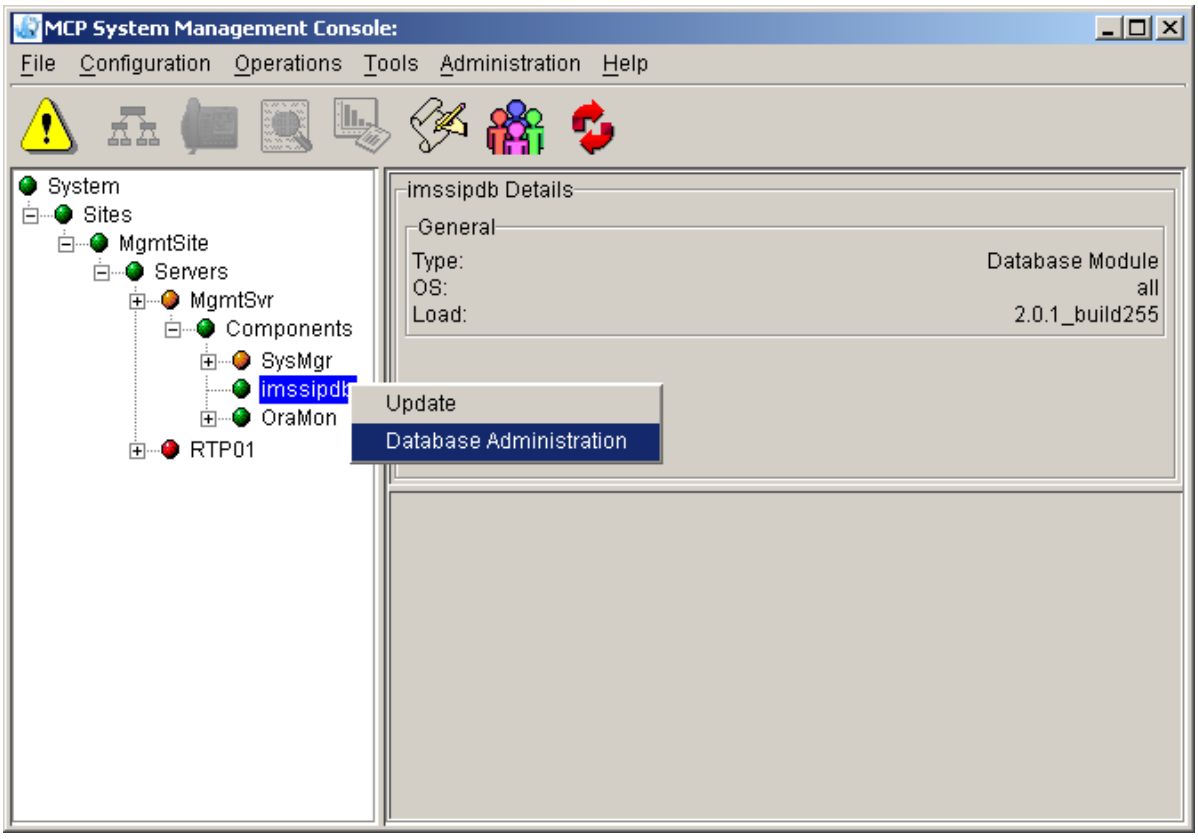
ATTENTION

Only users setup as database administrators or system administrators have access to the Database Administration option in the System Management Console.

From the System Management Console

1 In the System tree, select the Database Module component (**imssipdb**).

2 From the Administration menu, select the **Database Administration** command.



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

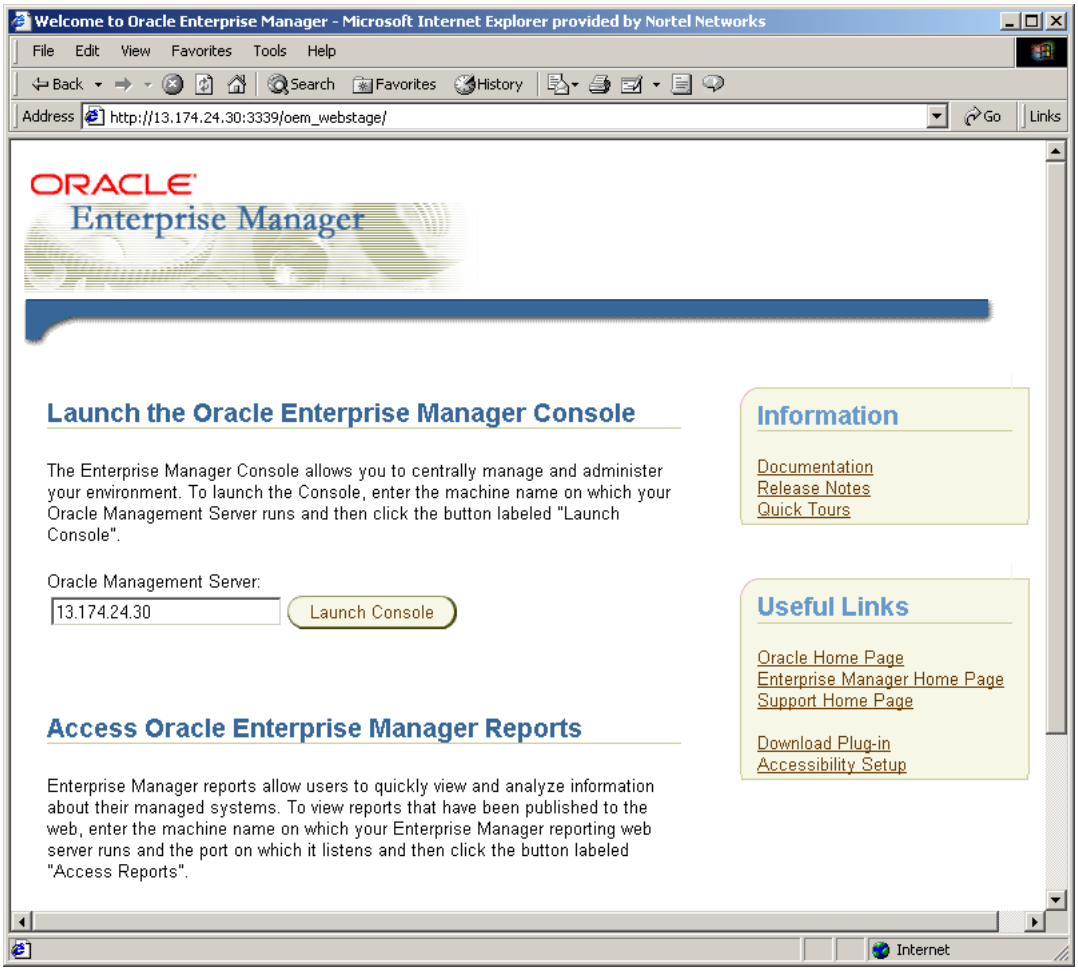
4 Enter the **imssipdb** database IP address provided during installation.

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

Note: Prior to launching the OEM Console for the first time (or after upgrading or changing web browsers), the administrator must first download the Oracle Jinitiator plug-in. This plug-in is required for all web browsers to work with the OEM Console.

To download the Oracle Jinitiator plug-in, select the **Download Plug-in** item under the **Useful Links** portion of the window. Follow the instructions for downloading and installing the Oracle Jinitiator plug-in.

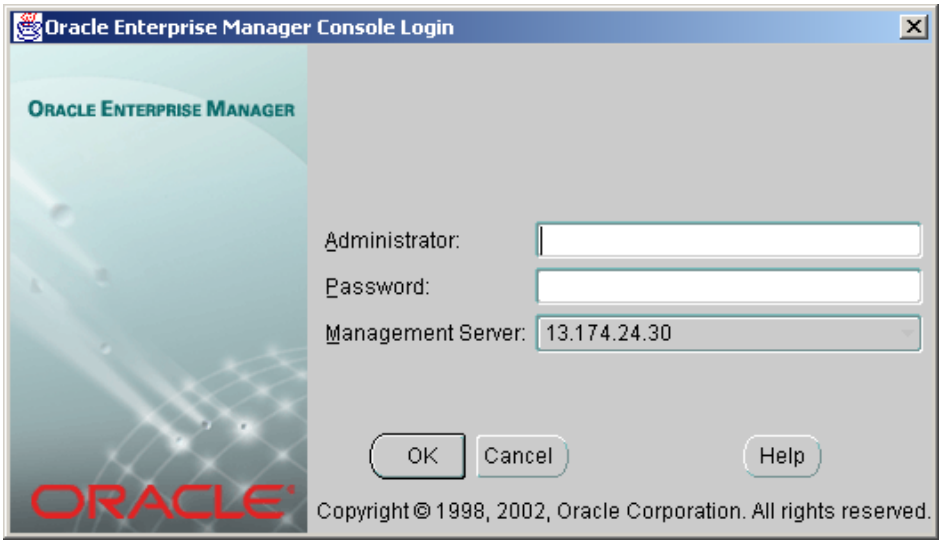
Figure 13 Launch the Oracle Enterprise Manager Console window



5 In the **Oracle Management Server** box shown in **step 3**, enter the IP address of the server hosting the primary database or the secondary database and click **Launch Console**.

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

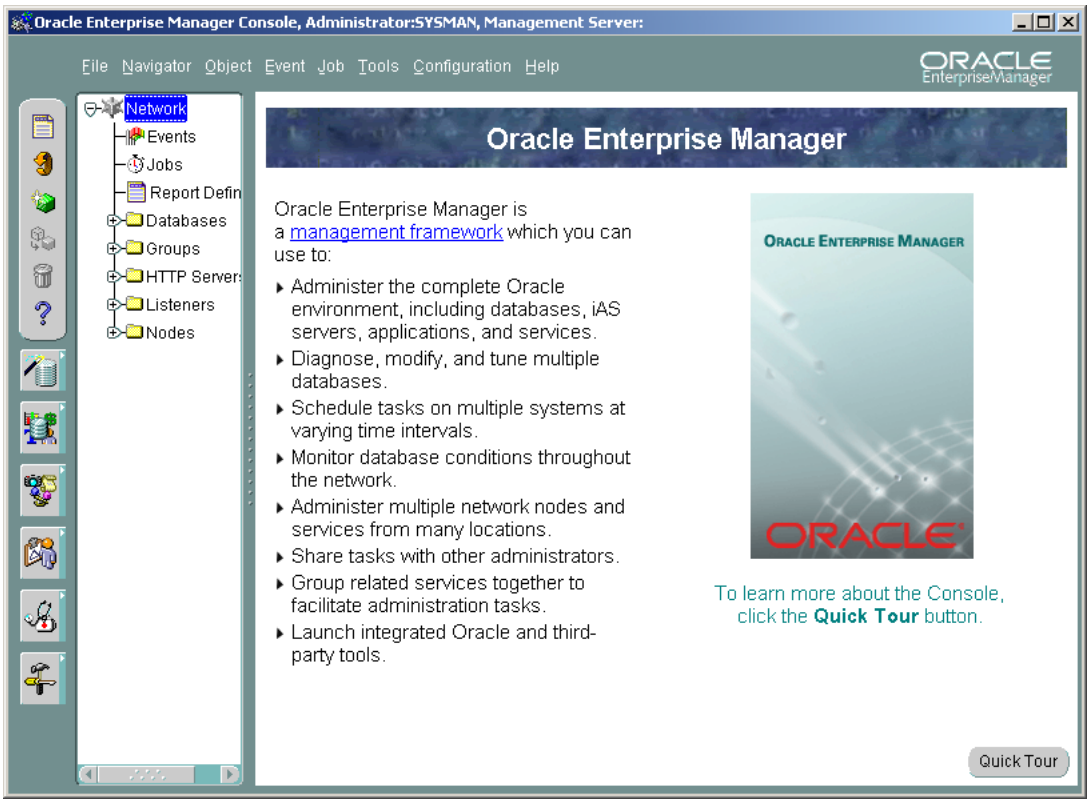
Figure 14 Oracle Enterprise Manager Console Login window



Note: If the OEM Console Login window does not appear, ensure that the Oracle Jinitiator plug-in has been installed, as described in the previous step.

6 Enter the **sysman** user name and password provided during installation and click **OK**.The **Oracle Enterprise Manager Console** opens as shown in Figure 15, Oracle Enterprise Manager Console, on page 76.

Figure 15 Oracle Enterprise Manager Console



Configuring sysman preferences

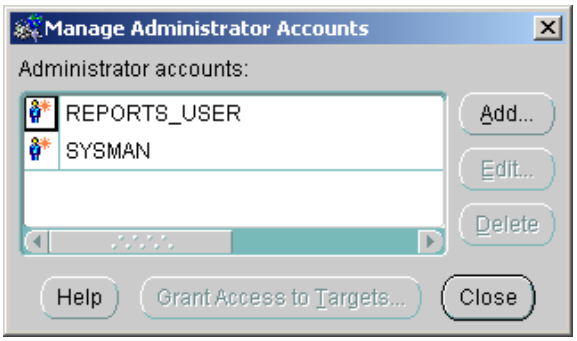
Use the following procedure to configure preferences for the **sysman** administrator:

From the OEM Console

1 From the **Configuration** menu, select **Manage Administrators**.

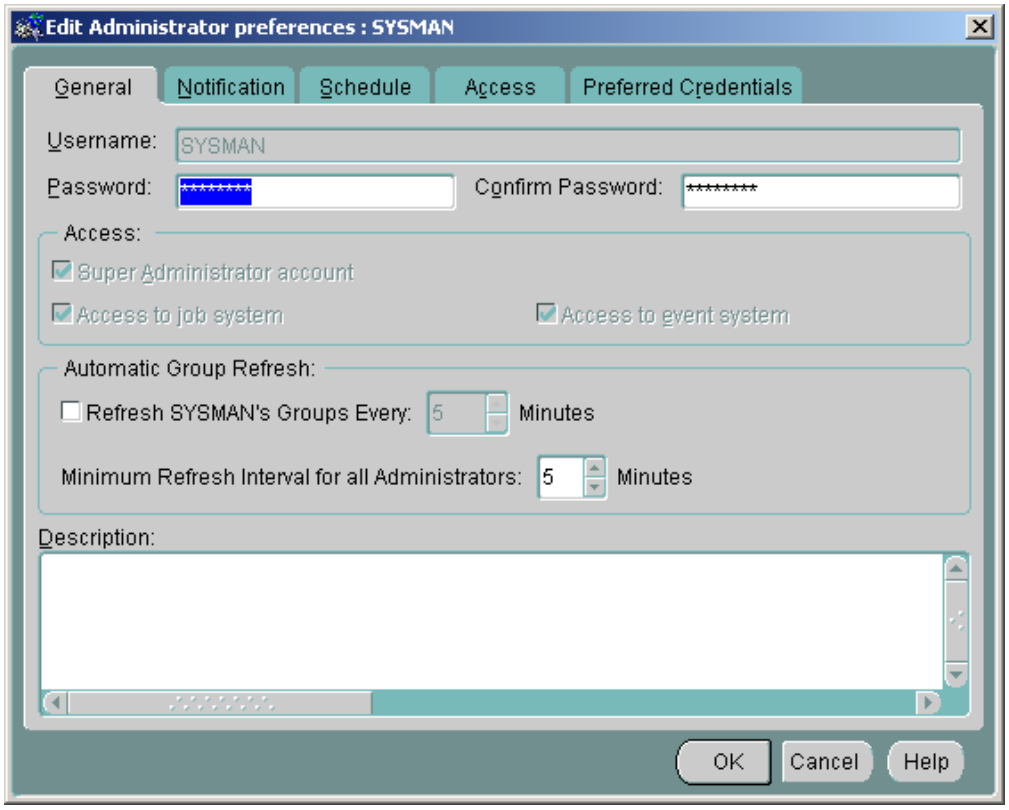
The **Manage Administrator Accounts** window opens as shown in Figure 16, Manage Administrator Accounts window, on page 77.

Figure 16 Manage Administrator Accounts window



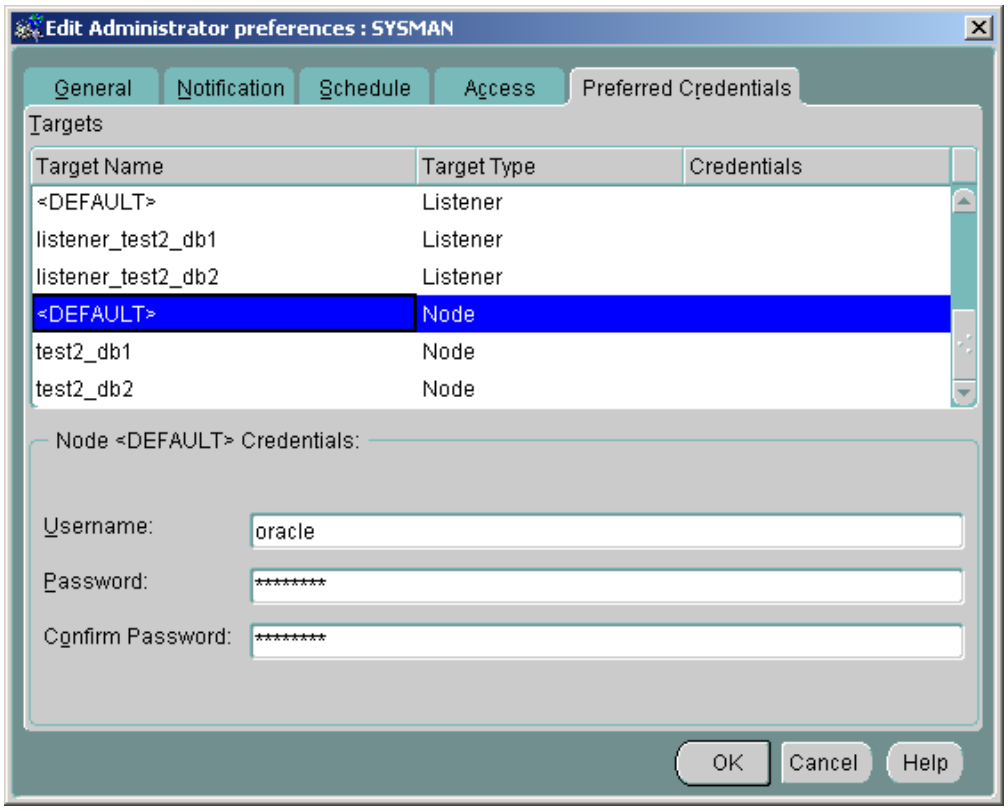
2 Select **sysman** and click **Edit**.

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



3 Select the **Preferred Credentials** tab.

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



4 Under **Targets**, select the **Target Name** and **Target Type** combination of <DEFAULT> and Node.

5 Enter the correct **Username** and **Password** for the **oracle** administrator and click **OK** to save all changes and close the **Edit Administrator Preferences** dialog box.

Configuring a database observer account

Observer accounts are used to allow users to only monitor the Oracle database(s).

Use the following procedure to set up observer accounts:

From the System Management Console

1 Launch the **Oracle Enterprise Manager Console** as described in Logging in to the OEM Console on page 73.

The **Oracle Enterprise Manager Console** Login window opens. Refer to Figure 14, Oracle Enterprise Manager Console Login window, on page 75.

2 Log in as **sysman** using the password supplied during installation.

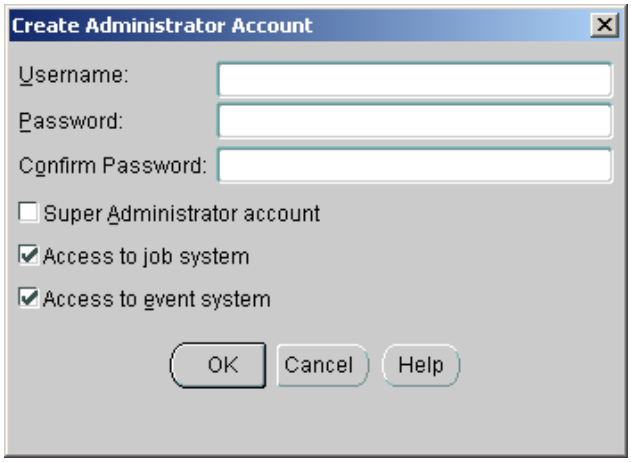
The **Oracle Enterprise Manager Console** opens. Refer to Figure 15, Oracle Enterprise Manager Console, on page 76.

3 From the **Configuration** menu, select **Manage Administrators**.

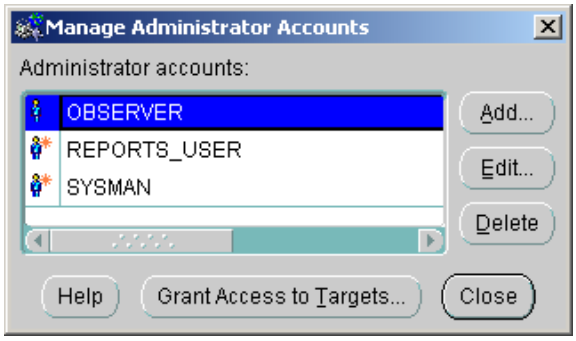
The **Manage Administrator Accounts** window opens. Refer to Figure 16, Manage Administrator Accounts window, on page 77.

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

The **Create Administrator Account** window opens.

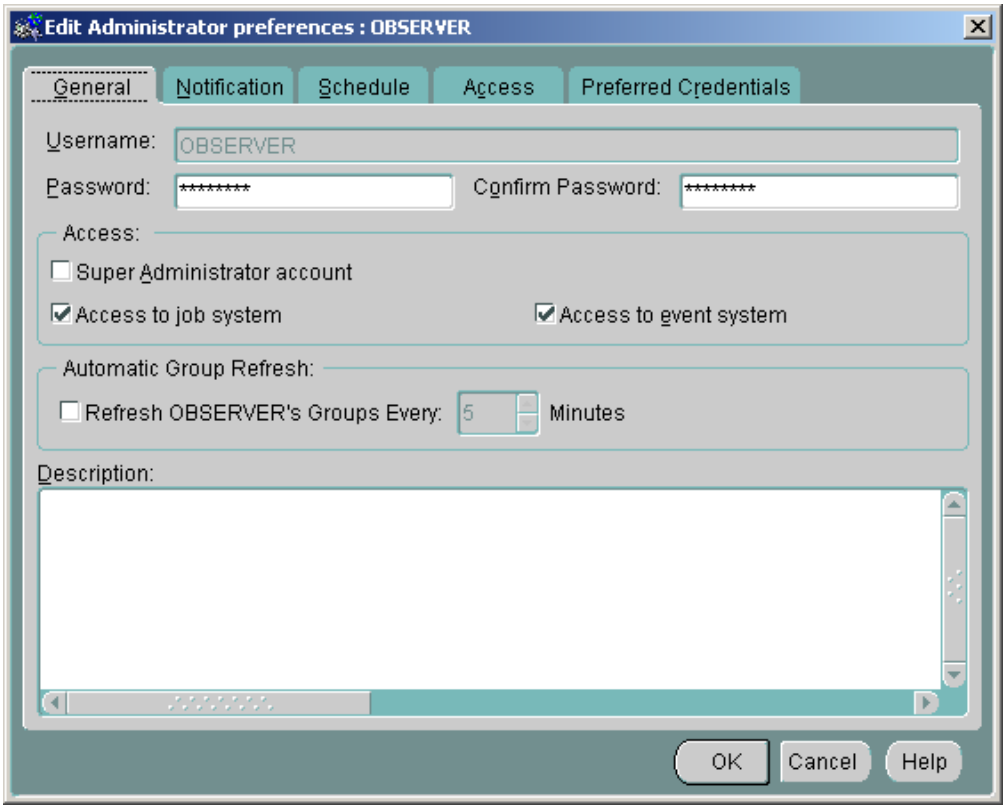


5 Enter **observer** and a password for the observer account and click **OK**. The observer administrator account will appear under **Administrator accounts:** field within the **Manage Administrator Accounts** window.



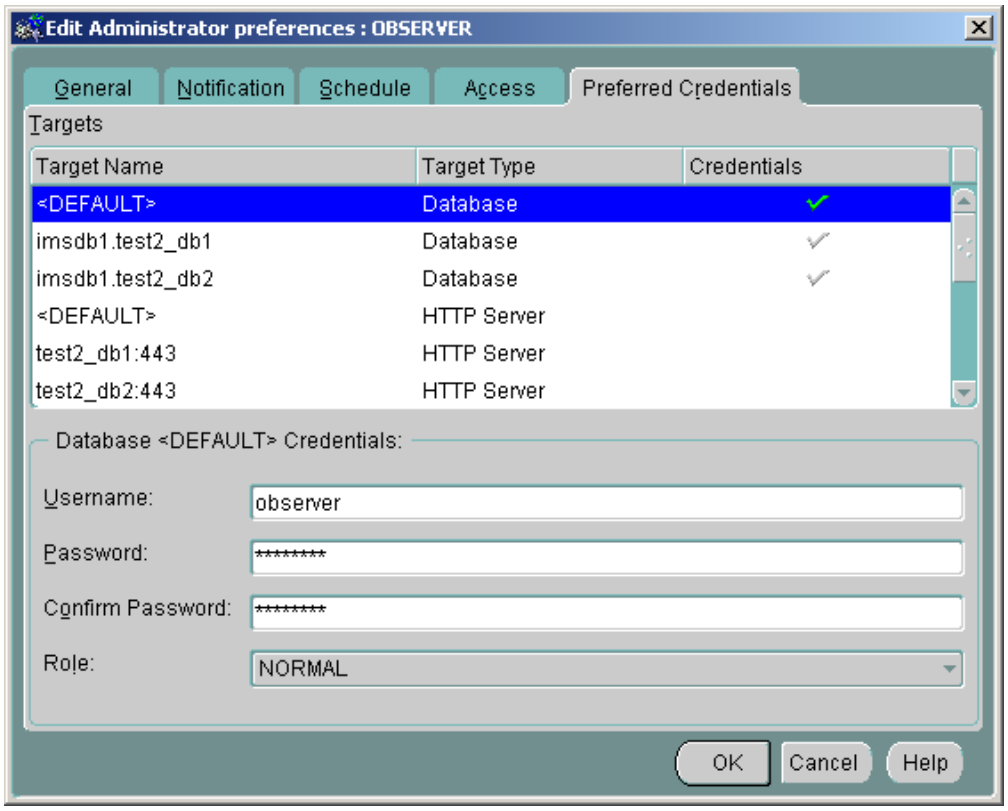
6 Select **observer** and click **Edit**.

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


Edit Administrator preferences : OBSERVER
General
Notification
Schedule
Access
Preferred Credentials
Username:
OBSERVER
Password:
****
Confirm Password:
****
Access:
Super Administrator account
Access to job system
Access to event system
Automatic Group Refresh:
Refresh OBSERVER's Groups Every:
5
Minutes
Description:
OK
Cancel
Help

7 Select the **Preferred Credentials** tab.

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



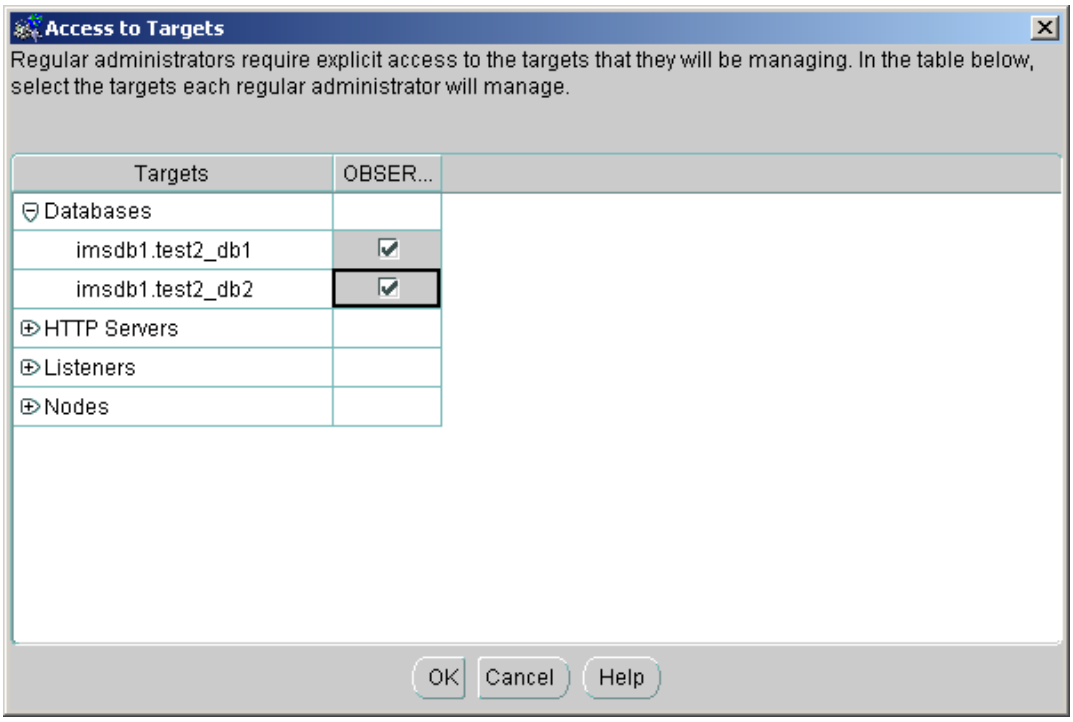
8 Under **Targets**, select the **Target Name** and **Target Type** combination of <DEFAULT> and Database.

9 Enter **observer** and the observer password provided during installation. Click **OK** to save all changes and close the **Edit Administrator Preferences** dialog box.

Note: The observer password entered above may not be the same as the password entered when creating the observer account.

10 Within the **Manage Administrator Accounts** window, select **observer** and click **Grant Access to Targets...**

The **Access to Targets** window opens.



11 Within the **Access to Targets** window, check the database targets that should be accessible by the observer administrator and click **OK**.

12 Click **Close** to close the **Manage Administrator Accounts** window.

Server configuration management

Configuring administrator roles

Only individuals with defined administrative roles have access to the system through the System Management Console. For more information on these administrator roles and their access privileges on the System Management Console, please refer to *CVoIP System Management Console User Guide*.

In order to configure and manage these administrators, a program is provided on the server hosting the primary database.

Starting administrator configuration program

Use the following procedure to start the program which provides access to configure and manage administrator information:

In a telnet window

1 Log in as **oracle** to the server hosting the primary database.

2 Start the program for configuring administrator roles by executing the following commands:

cd /IMS/imssipdb/data/db_schema/util

./mcp_cfgUser.pl

3 Enter the system administrator username and password at the appropriate prompts.

4 The following menu appears:

```
Select a option from the following list
 [1]  Add GenAdmin
 [2]  Delete GenAdmin
 [3]  Modify GenAdmin Password
 [4]  List current GenAdmins
 [5]  Modify SysAdmin Password
 [6]  Modify SysAdmin Username
 [7]  Quit
Please enter the number [1 to 7] of the
operation to perform :
```

This is the main menu for performing any configuration management for administrators, as described in the following sections.

Adding a general administrator

Use the following procedure to create a general administrator:

In a telnet window

1 Start the program for configuring administrator roles as described in Starting administrator configuration program on page 83.

2 From the main menu prompts:

```
Please enter the number [1 to 7] of the
operation to perform :
```

enter **1** in order to add a general administrator.

Note: Only 20 general administrators are allowed for the system. If the user attempts to add more than 20 general administrators, an error message is displayed to the user.

3 Enter the username and password for the new general administrator at the appropriate prompts.

Note: Usernames and passwords have the following restrictions:

- The new username must be unique compared to all other administrator usernames.
- Usernames must be between 2 and 24 characters in length.
- Passwords must be between 5 and 24 characters in length.
- Only the following characters are allowed within usernames and passwords:
  - Characters A through Z
  - Characters a through z
  - Numeric characters 0 through 9
  - Period character (’.’)
  - Hyphen character (’-’)
- Only three attempts to enter a valid username is allowed. After the third attempt, the operation is aborted and the user is returned to the main menu. A valid username is considered to be a username which conforms to the length and character restrictions listed above.
- Only three attempts to enter a valid password is allowed. After the third attempt, the operation is aborted and the user is returned to the main menu. A valid password is considered to be a password which conforms to the length and character restrictions listed above.
- Only two attempts to confirm the password is allowed. After the second attempt, the operation is aborted and the user is returned to the main menu.

4 A success message is displayed to the user and the user is returned to the main menu.

5 Perform other configuration management operations as described in the subsections of Configuring administrator roles on page 83.

Deleting a general administrator

Use the following procedure to delete an existing general administrator:

In a telnet window

1 Start the program for configuring administrators as described in Starting administrator configuration program on page 83.

2 From the main menu prompts:

```
Please enter the number [1 to 7] of the
operation to perform :
```

enter **2** in order to add a general administrator.

3 A menu appears listing all of the administrator usernames. At the administrator list prompt

```
Please enter the number [1 to X] of the user to
delete :
```

enter the number corresponding to the general administrator to be deleted.

4 At the confirmation prompt, confirm the username of the general administrator to be deleted by entering **Y**.

5 A success message is displayed to the user and the user is returned to the main menu.

6 Perform other configuration management operations as described in the subsections of Configuring administrator roles on page 83.

Modify a general administrator password

Use the following procedure to modify an existing general administrator's password:

In a telnet window

1 Start the program for configuring administrators as described in Starting administrator configuration program on page 83.

2 From the main menu prompts:

```
Please enter the number [1 to 7] of the
operation to perform :
```

enter **3** in order to modify a password for a general administrator.

3 A menu appears listing all of the administrator usernames. At the administrator list prompt

```
Please enter the number [1 to X] of the user to
modify :
```

enter the number corresponding to the general administrator to be modified.

4 Enter the new password for the general administrator at the appropriate prompts.

Note: Valid passwords must conform to the following restrictions:

- Passwords must be between 5 and 24 characters in length.
- Only the following characters are allowed within passwords:
  - Characters A through Z
  - Characters a through z
  - Numeric characters 0 through 9
  - Period character (’.’)
  - Hyphen character (’-’)
- Only three attempts to enter a valid password is allowed. After the third attempt, the operation is aborted and the user is returned to the main menu.
- Only two attempts to confirm the password is allowed. After the second attempt, the operation is aborted and the user is returned to the main menu.

5 A success message is displayed to the user and the user is returned to the main menu.

6 Perform other configuration management operations as described in the subsections of Configuring administrator roles on page 83.

List all general administrators

Use the following procedure to list all existing general administrators:

In a telnet window

1 Start the program for configuring administrators as described in Starting administrator configuration program on page 83.

2 From the main menu prompts:

```
Please enter the number [1 to 7] of the
operation to perform :
```

enter **4** in order to list all the current general administrators.

3 A menu appears listing all of the administrator usernames and the user is returned to the main menu.

4 Perform other configuration management operations as described in the subsections of Configuring administrator roles on page 83.

Modify the system administrator password

Use the following procedure to modify the system administrator's password:

In a telnet window

1 Start the program for configuring administrators as described in Starting administrator configuration program on page 83.

2 From the main menu prompts:

```
Please enter the number [1 to 7] of the
operation to perform :
```

enter **5** in order to modify the password for the system administrator.

3 Enter the new password for the system administrator at the appropriate prompts.

Note: Valid passwords must conform to the following restrictions:

- Passwords must be between 5 and 24 characters in length.
- Only the following characters are allowed within passwords:
  - Characters A through Z
  - Characters a through z
  - Numeric characters 0 through 9
  - Period character ('.')
  - Hyphen character ('-')
- Only three attempts to enter a valid password is allowed. After the third attempt, the operation is aborted and the user is returned to the main menu.
- Only two attempts to confirm the password is allowed. After the second attempt, the operation is aborted and the user is returned to the main menu.

4 A success message is displayed to the user and the user is returned to the main menu.

5 Perform other configuration management operations as described in the subsections of Configuring administrator roles on page 83.

Modify the system administrator username

Use the following procedure to modify the system administrator's username:

In a telnet window

1 Start the program for configuring administrators as described in Starting administrator configuration program on page 83.

2 From the main menu prompts:

```
Please enter the number [1 to 7] of the
operation to perform :
```

enter **6** in order to modify the username for the system administrator.

3 Enter the new username for the system administrator at the appropriate prompts.

Note: Valid usernames must conform to the following restrictions:

- Usernames must be between 2 and 24 characters in length.
- Only the following characters are allowed within usernames:
  - Characters A through Z
  - Characters a through z
  - Numeric characters 0 through 9
  - Period character ('.')
  - Hyphen character ('-')
- Only three attempts to enter a valid username is allowed. After the third attempt, the operation is aborted and the user is returned to the main menu.

4 A success message is displayed to the user and the user is returned to the main menu.

5 Perform other configuration management operations as described in the subsections of Configuring administrator roles on page 83.

Quitting administrator configuration program

Use the following procedure to quit the administrator configuration program:

In a telnet window running the program

1 From the main menu prompts:

```
Please enter the number [1 to 7] of the
operation to perform :
```

enter **7** to quit the program.

Upon quitting this program, a path to a log file for that session is provided. In order to distinguish different program session log files, the following file naming convention is used:

`mcp_cfgUser.pl.log.<date>.<time>`

where:

`<date>` is the date the file was created in <year>_<month>_<day> format

For example, `2002_3_9` represents March 9, 2002

`<time>` is the time the file was created in <hour>:<minute>:<second> format

For example, `22:15:28` represents 10:15 p.m. and 28 seconds.

Accounting management

Functional description

The Database functionality does not perform any accounting management.

Performance management

Functional description

Database logs, alarms, and operational measurements are displayed in the System Management Console. For details, please refer to *CVoIP System Management Console User Guide*.

Operational measurements

Operational measurements consist of counters and gauges monitoring the activity of the Oracle database processes. The Oracle Monitor component generates OMs for the following groups:

- DBUsage/OracleServer
- IMS Main Database_TableSpace
- DataFile
- IMS Main Database_DiskSpace
- Oracle Server
- DBAccess
- Oracle Listeners_Listener
- IMS Main Database

Operational measurement files generated by the Oracle Monitor are viewed using System Management Console OM browsers. The current OM file is viewed in the Active OM Browser. After the configured interval or file size, the active OM file is rotated out, going from an active to holding status.The holding files are viewable in the Holding Log Browser until the file retention period expires.

DBUsage/OracleServer

This OM group contains various measurements used to support database activities of current sessions on the managed element.This

information has been found to be particularly useful for monitoring global database instance performance.

Table 22 DBUsage/OracleServer

Performance measurement	Definition
BlockGetsPerSec	This ratio determines the block get rate. The block get rate is a basic measure of the rate at which the application system references the database. (oraDbSysConsistentGets + oraDbSysDbBlockGets) / time unit
CacheHitRatio_Percent	This ratio measures the effectiveness of the buffer cache. The normally acceptable range is 70 - 85%. (oraDbSysConsistentGets + oraDbSysBlockGets - oraDbSysPhysReads) / (oraDbSysConsistentGets + oraDbSysBlockGets)

IMS Main Database_TableSpace

A tablespace is a logical portion of an Oracle database instance used to allocate storage for table and index data. In a production environment, tables can fill up as transaction activity mounts. Monitoring tablespace activity is important to avoid exhausting the tablespaces and causing spaces. Each tablespace represents a given tablespace within a current database instance.

An example is the SYSTEM table space. It contains all the database information. If lost, corrupted or full, the database will not function properly or not function at all

Table 23 IMS Main Database_TableSpace

Performance measurement	Definition
SizeAllocated_KBytes	Indicates the amount of disk space (in kilobytes) allocated for this tablespace. This is the sum of the sizes of the data files associated with the tablespace.
SizeUsed_KBytes	Indicates the amount of disk space (in kilobytes) which is actually in use for storing data. This is the difference between the sum of the size of the datafiles associated with the tablespace and the sum of the size of the free spaces associated with the tablespace.

Table 23 IMS Main Database_TableSpace

Performance measurement	Definition
State	(1) online (2) offline, or (3) invalid Indicates the current accessibility of this tablespace. If a tablespace is offline (2), then SQL statements cannot reference objects contained in the tablespace. An invalid (3) tablespace is one that has been dropped.
PercentageUtilization	Percentage table space used.
PercentageUtilization_ Min	Minimum table space percentage utilization seen by monitor while monitor has been running.
PercentageUtilization_ Max	Maximum table space percentage utilization seen by monitor while monitor has been running.

DataFile

A data file denotes an area of disk allocated for database data. Monitoring data files is important for two reasons: first, to determine whether space in files is being exhausted, and second to determine operating system response time in accessing data on disk, especially on platforms where there is no other way to measure disk queue length. Each DataFile represents a given data file within a current database instance on the node.

Tablespace is logical space allowed by the database to contain the data. A tablespace is made up of one or more data files. Note that different data files can be stored on different disks.

Table 24 DataFile

Performance measurement	Definition
Allocated_KBytes	Indicates the allocated size (in kilobytes) of this data file. Indicates how much space has been used so far. Monitoring this variable is very important, because running out of space can require taking the database down, depending on which table this file supports. Normally, however, adding another data file to the Tablespace solves the problem.

Table 24 DataFile

Performance measurement	Definition
Disk_Reads	Indicates the total number of reads issued against this data file since database instance startup.
Disk_Writes	Indicates the total number of writes issued against this data file since database instance startup.

IMS Main Database_DiskSpace

This OM group contains general information about an actively opened database instance on the managed element.

Table 25 IMS Main Database_DiskSpace

Performance measurement	Definition
SizeUnit	Displays the units used to measure the size of this database instance, as indicated by the values for SizeAllocated and SizeUsed. The value of SizeUnits is the least that allows SizeAllocated to be expressed as a 32-bit integer. (1) bytes, indicates size measured in bytes; (2) kbytes, indicates units of kilobytes; (3) mbytes, indicates units of megabytes; (4) gbytes, indicates units of gigabytes; or (5) tbytes, indicates units of terabytes. Each of these unit measurements are binary multiples (1K = 1024)
AllocatedDisk	Displays the estimated size of this database instance, which is the disk space that has been allocated to it and is no longer available to users on this host. The SizeAllocated does not necessarily indicate the amount of space actually in use for database data; SizeUsed retrieves this value instead. The value of this variable is the sum of the BYTES field for the rows of the DBA_DATA_FILES tables.
UsedDisk	Displays the estimated size of this database instance actually in use for database data. The value of SizeUsed is the sum of values in the BYTES field of DBA_DATA_FILES minus the sum of values in the BYTES field of DBA_FREE_SPACE. SizeUsed should always be less than or equal to SizeAllocated.
PercentUtilization	Percentage of disk used.

Table 25 IMS Main Database_DiskSpace

Performance measurement	Definition
PercentUtilization_Min	Minimum percentage utilization seen by monitor during lifetime of monitor.
PercentUtilization_Max	Maximum percentage utilization seen by monitor during lifetime of monitor.

Oracle Server

This OM group contains operation status about each database server actively running on the managed element.

Table 26 Oracle Server

Performance measurement	Definition
ServerOpStatus	The UP value (1) indicates that the server is operational and available. The DOWN value (2) indicates that the server is not available.

DBAccess

This OM group contains information about each database server actively running on the managed element.

Table 27 Oracle Server

Performance measurement	Definition
Disk_Reads	Displays the total number of reads of database files this server has issued to the operating system since startup of this database server instance.
Disk_Writes	Displays the total number of writes of database files
Logical_Reads	Displays the total number of logical reads of database files that this server has made internally since startup. This value and the value of DiskReads reveal the effect of caching on read operations.
logical_Writes	Displays the total number of logical writes

Oracle Listeners_Listener

The name of the generic listener, as retrieved from the LISTENER.ORA configuration file. This listener represents the network listener for a current database instance on the server.

Table 28 Oracle Listeners_Listener

Performance measurement	Definition
State	Indicates the state of the listener; a value of 1 indicates that the listener is up and a 2 indicates that the listener is down.
Trace Level	Indicates the level at which a Listener should be traced. A value of 4 means that tracing at the USER level is turned on; and 6 means that tracing at the ADMIN level is turned on. A value of 17 means that tracing is turned off.

IMS Main Database

Table 29 IMS main database

Performance measurement	Format	Definition
OracleDBSNMPConnection LostCount	Integer	Number of lost connections to the Oracle SNMP agent during the collection period.
OracleDBSNMPError ResponseCount	Integer	Number of error responses received from the Oracle SNMP agent during the collection period.
OracleDBSNMPTimeOut ResponsesCount	Integer	Number of time out responses received from the Oracle SNMP agent during the collection period.
DB_OPStatus	Integer	Operation status of the Database (a value of 2 is "normal").

Security and Administration

How this chapter is organized

This chapter is organized as follows:

Security

The Database functionality uses Oracle database technology to ensure confidentiality, integrity, and availability of data. All configuration data held in the Oracle database 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 30, Database administrator and user roles, on page 99 describes user accounts used to administer the Database functionality.

Table 30 Database administrator and user roles

Username	User type	Description
oracle	UNIX user	Runs command line scripts on the server(s) hosting the Oracle database(s).
sysman	OEM user	Manages administration of the database from the OEM Console.
observer	OEM user	Observers and monitors the database from the OEM Console
imsdba	Database user	Owns the schema used by MCS network components.
repadmin	Database user	Performs replication maintenance operations.
observer	Database user	Provides observer access to the database.

Administration

Functional description

Database administration consists of registering events, creating backup jobs, and recovery for the Oracle database(s). It also includes the option to generate reports to display information about the Oracle database(s).

Events

As certain database events occur, alerts are raised on the OEM console in order to notify the database administrator that the event was encountered. Table 31, Recommended database events, on page 100 lists the recommended Oracle database event types and descriptions

of each. It is recommended that all of the events listed be registered on the Oracle database(s) through the OEM Console.

Table 31 Recommended database events

Events	Type	Description
Alert	Fault	New errors are shown in the **alert<DBname>.log** file, where **DBname** is the name of the database within the OEM Console.
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.

Table 31 Recommended database events

Events	Type	Description
Alert File Large	Space	The alert file is too large.
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.

Database backup

The OEM Console supports scheduling automated backups of the Oracle database as often as required.

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

CAUTION

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

The recommended backup method for taking backups of the Oracle database is the Export/Import backup method. This backup method provides the ability to backup an Oracle database by taking a complete export of the data in an Oracle database rather than incremental backups.

If a backup fails, the job output display the probable cause of the failure and any available explanatory information. To view the job output, double-click a failed job displayed in the OEM Console. For more information, refer to Monitoring database backup jobs on page 35.

Reports

Reports can be generated from the OEM Console to display information about configuration, current status, events, and backup jobs.

It is recommended that the database administrator generate the reports listed in Table 32, Recommended database reports, on page 102.

Table 32 Recommended database reports

Report Title	Category	Description
Storage – Configuration	Configuration	Displays status and size of all storage objects
Database Object Space Usage	Current Status	Shows space usage reports for database objects
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

Table 32 Recommended database reports

Report Title	Category	Description
Registered Events Sorted by Target	Event	Provides information, sorted by target, for all registered events
Replication (only in a redundant architecture)	Configuration	Shows detailed configuration and statistics of a replicated system

Tools and utilities

The Database functionality uses the following administrative tools:

- **Oracle Enterprise Manager (OEM) Console:** Used by the database administrator for administration of database related events, jobs, and reports.

Tasks

Table 33, Administration task flows, on page 103 outlines Database administration tasks.

Table 33 Administration task flows

Topic	Subtopic	Procedure
Events	Registering/Scheduling Events	Creating an Export/Import Oracle database backup job on page 109
Database backups	Export/Import	Creating an Export/Import Oracle database backup job on page 109
	Export/Import	Modifying a scheduled Export/Import Oracle database backup job on page 114
Database recovery	Export/Import	Restoring exported Oracle database backup files on page 117

Table 33 Administration task flows

Topic	Subtopic	Procedure
	Control files	Restoring control files on page 118
Reports	Generation	Generating reports on page 120

It is recommended that all the configuration tasks listed in Configuration management on page 61 be completed prior to performing any of the administration tasks listed above.

Registering an Oracle database event

In order to receive alerts, administrators must register a database event with the Oracle database(s) through the OEM Console.

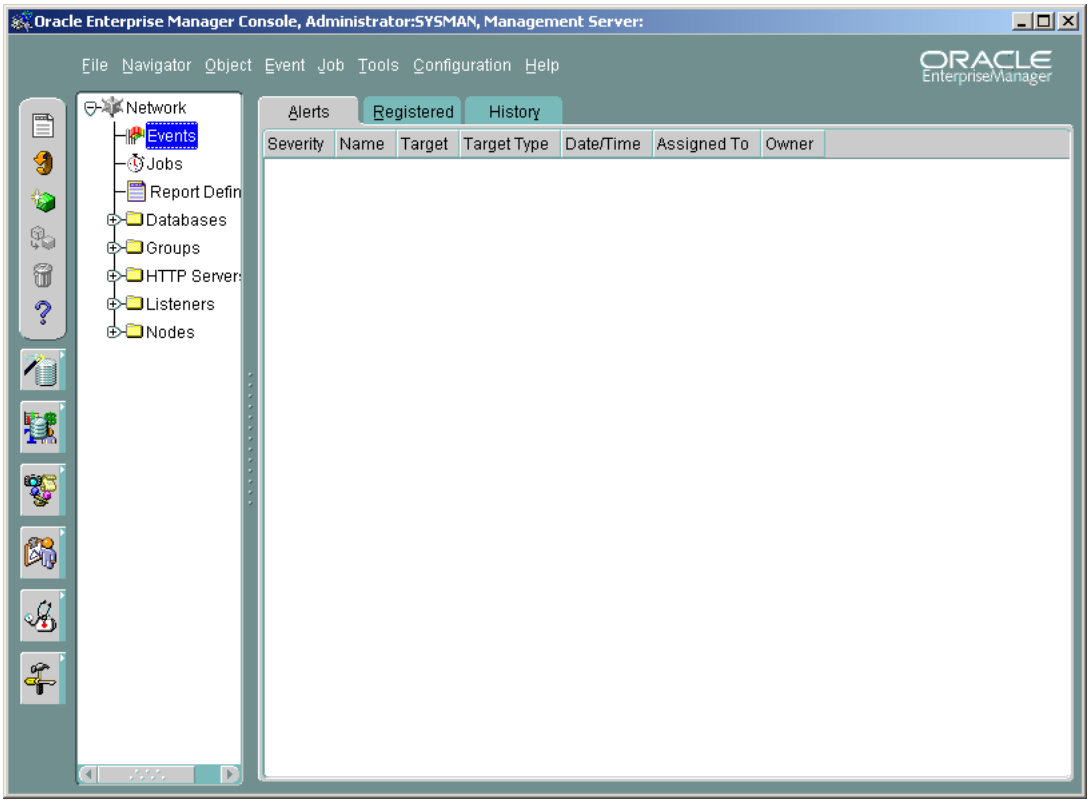
Creating an Oracle database event

Use the following procedure to create/register database events on the OEM Console:

Set general event properties

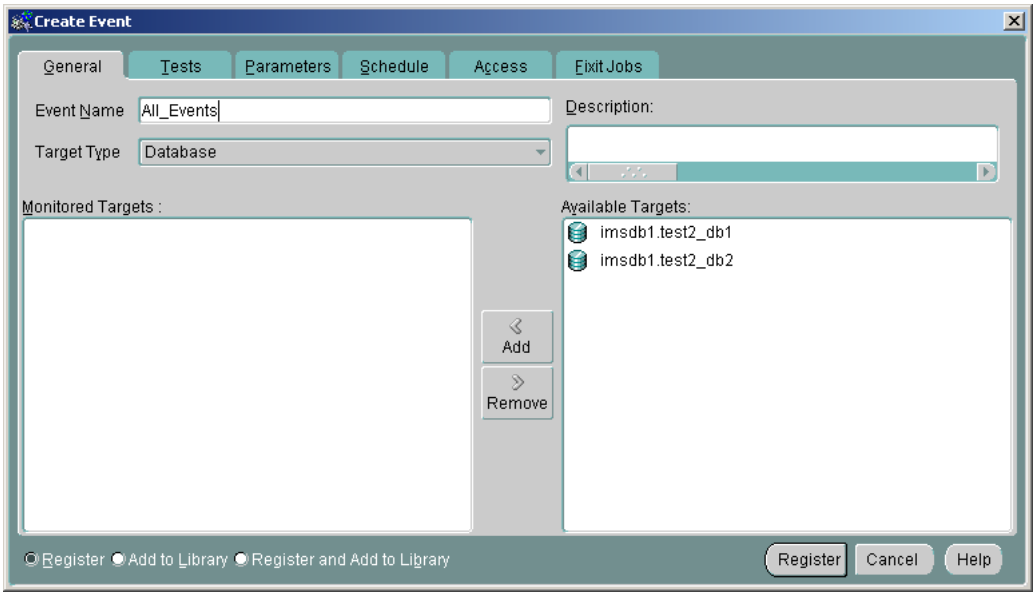
1 From the **Network** tree, select **Events**.

The **Events > Alerts** pane displays the list of active alerts.



2 From the **Event** menu, select **Create Event**.

The **Create Event > General** pane opens.

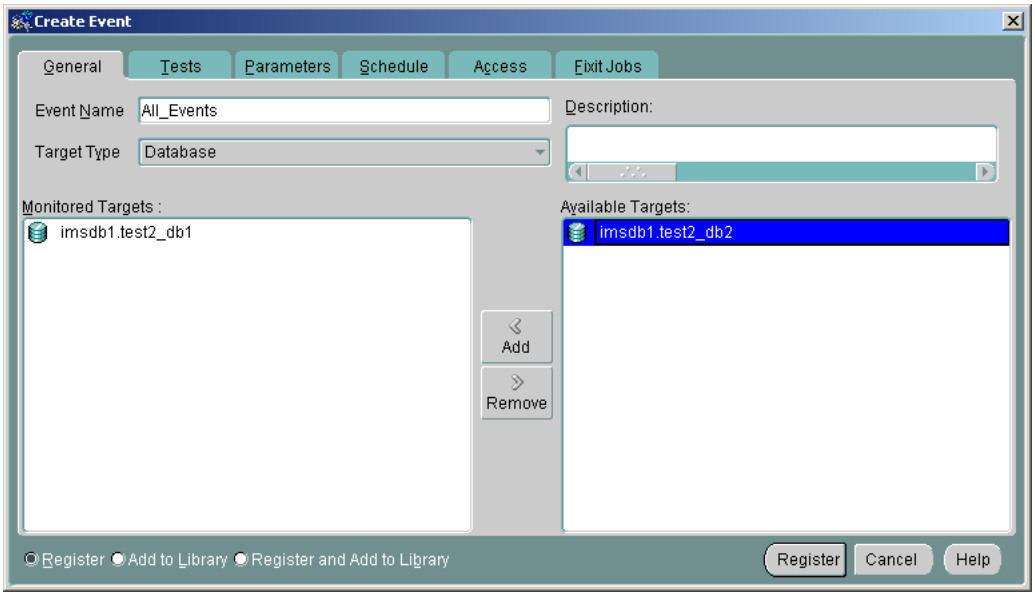


3 In the **Event Name** box, type a name to associate with the group of events being registered.

4 Under **Target Type**, select **Database**.

5 In the **Available Targets** box, select the node name where the primary Oracle database resides and click **Add**.

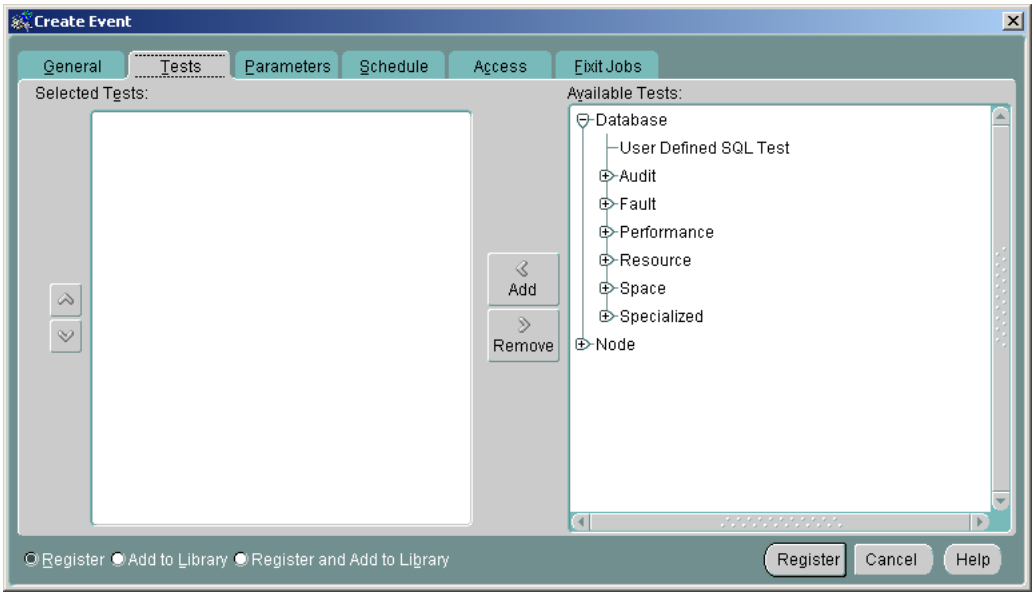
The target node name which was selected moves into the **Monitored Targets** list.



Select the tests/events

6 Click the **Tests** tab.

The **Create Event > Tests** pane opens.



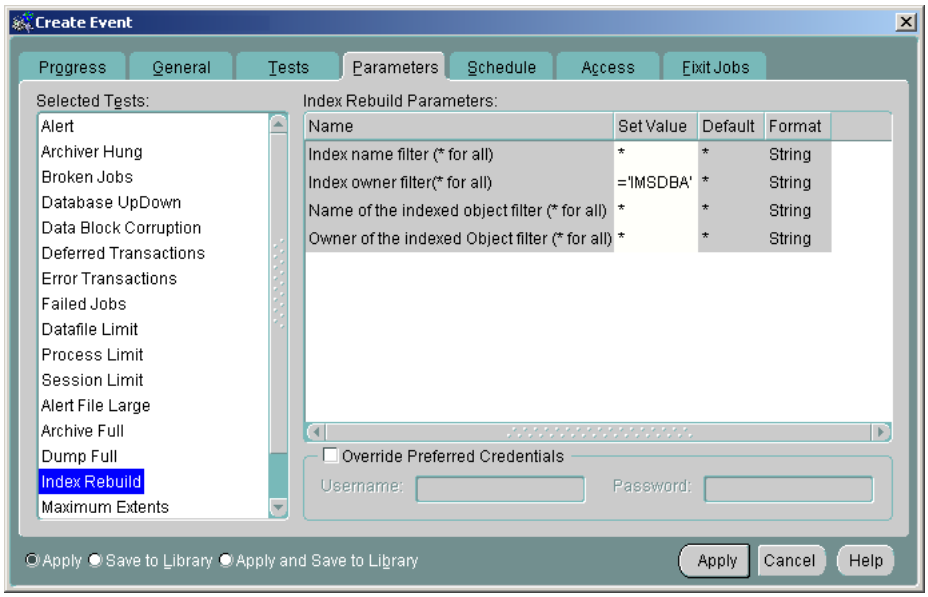
7 In the **Available Tests** box, select, from within the groupings, one of the recommended events listed in Events on page 99. Click **Add**.

The selected event is added to the **Selected Tests** box. Repeat this step for all the recommended events.

Define test parameters

8 Click the **Parameters** tab.

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



9 In the **Selected Tests** box, select the **Index Rebuild** test.

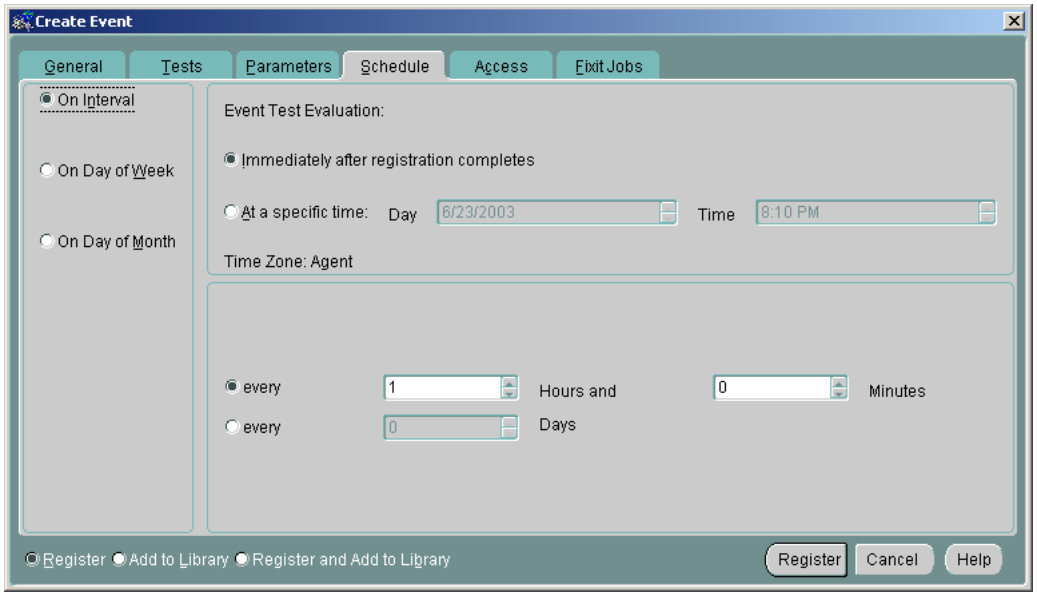
10 In the **Index Rebuild Parameters** box, enter **='IMSDBA'** within the **Set Value** column for **Index owner filter**.

Note: Only the **Index owner filter** parameter of the **Index Rebuild** test is required to be modified. All other test properties are automatically set to their corresponding default values.

Schedule event test frequency

11 Click the **Schedule** tab.

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



12 Select **On Interval**. Next, set the **every** option for 1 hour and 0 minutes.

Register and add the event group to the library

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

a Select the **Register and Add to Library** option.

b Click the **Register and Add** button to save the event.

The **Create Event** dialog box closes and the new event appears in the **Events > Registered** tab.

14 In a redundant architecture, repeat this entire process for the secondary Oracle database.

Oracle database backups using Export/Import

Database backups is achieved by scheduling backups of the primary Oracle database through the OEM Console.

Use the procedures listed in this section to schedule or modify existing scheduled backups using the Export/Import backup method.

Creating an Export/Import Oracle database backup job

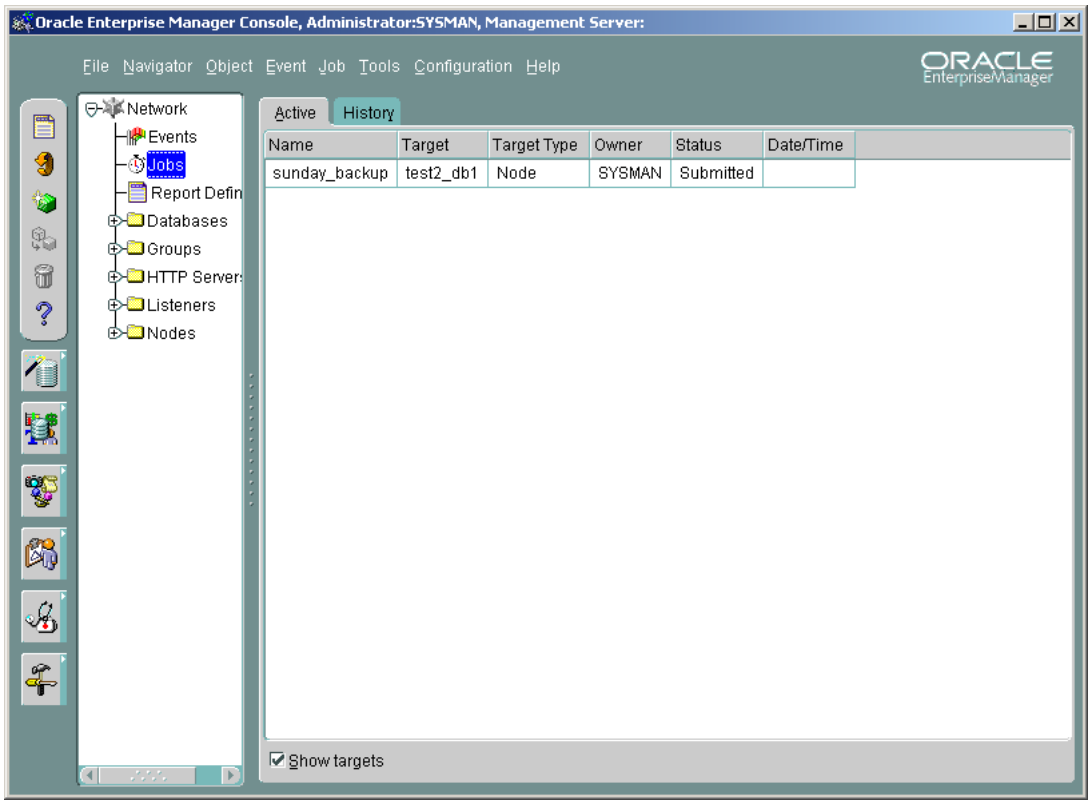
Use the following procedure to create backup jobs from the OEM Console using the Export/Import backup method:

Note: When a scheduled backup job is run, the approximate export time is 25 MegaBytes of data per minute.

Set general backup properties

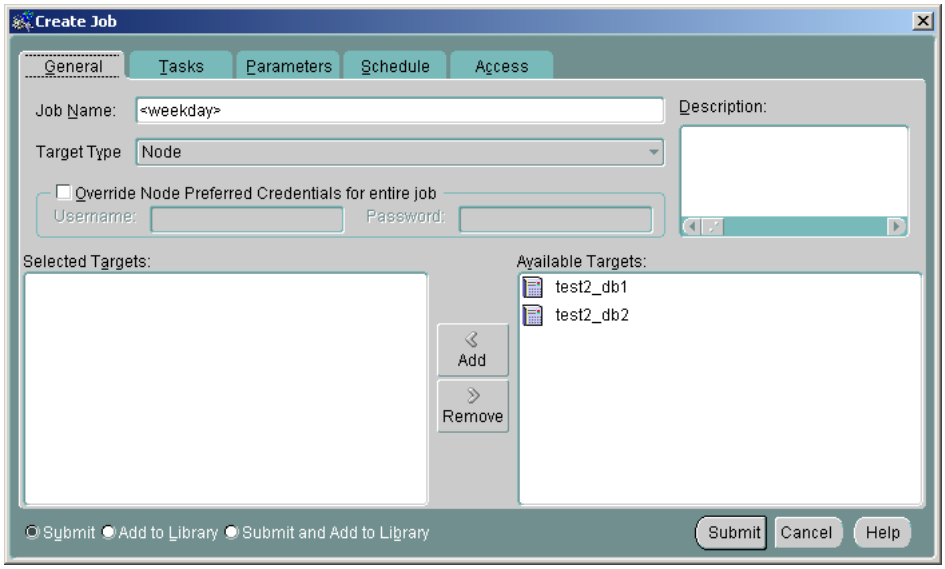
1 From the **Network** tree, select **Jobs**.

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.

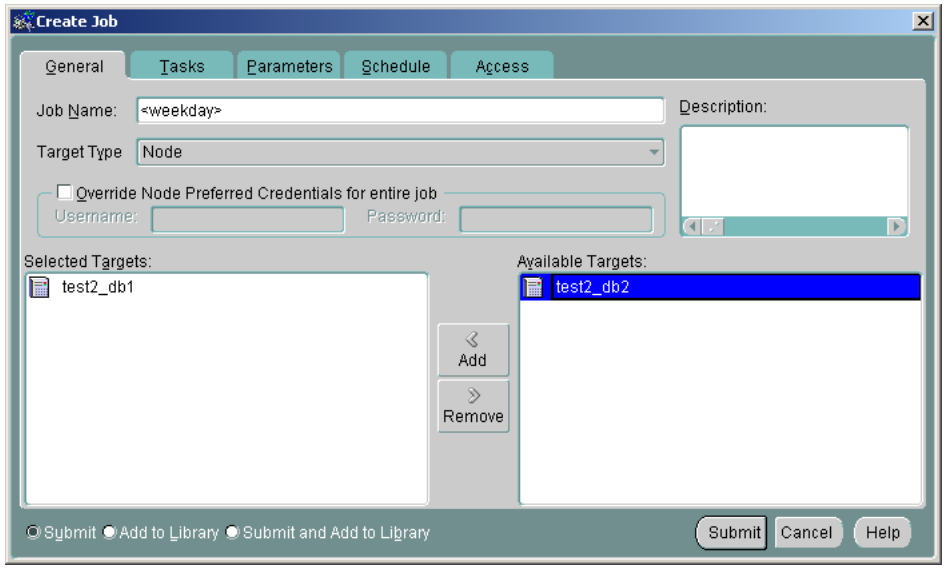


3 In the **Job Name** box, type **<weekday>**, where **weekday** is the day of the week the job should be run.

4 Under **Target Type**, select **Node**.

5 In the **Available Targets** box, select the node name where the primary Oracle database resides and click **Add**.

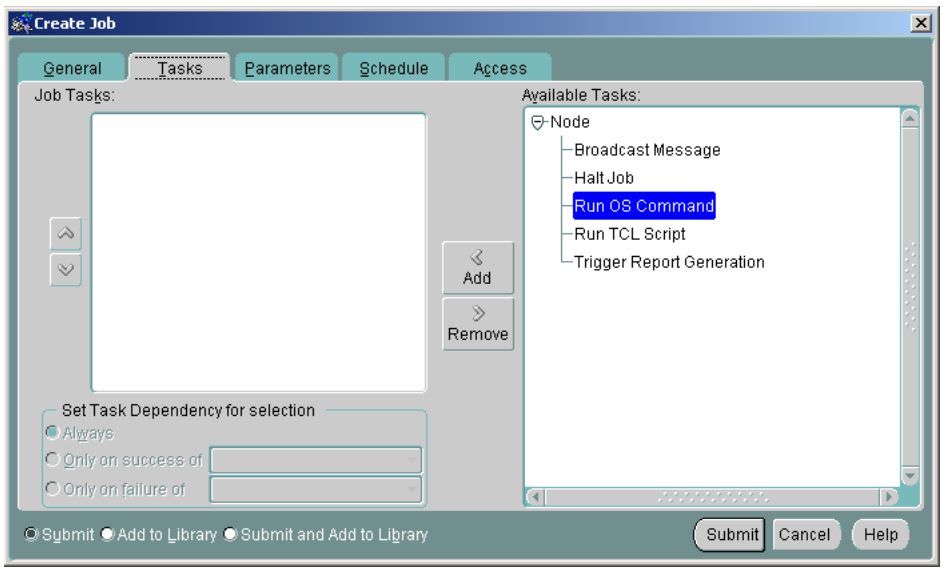
The target node name which was selected moves into the **Selected Targets** list.



Set backup task properties

6 Click the **Tasks** tab.

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



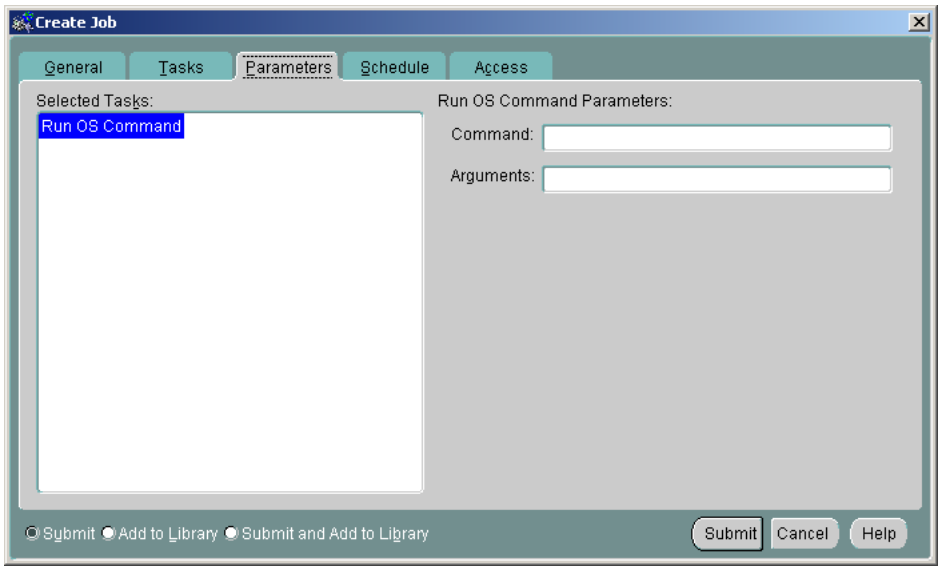
7 Select **Run OS Command** from the **Available Tasks** pane and click **Add**.

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.



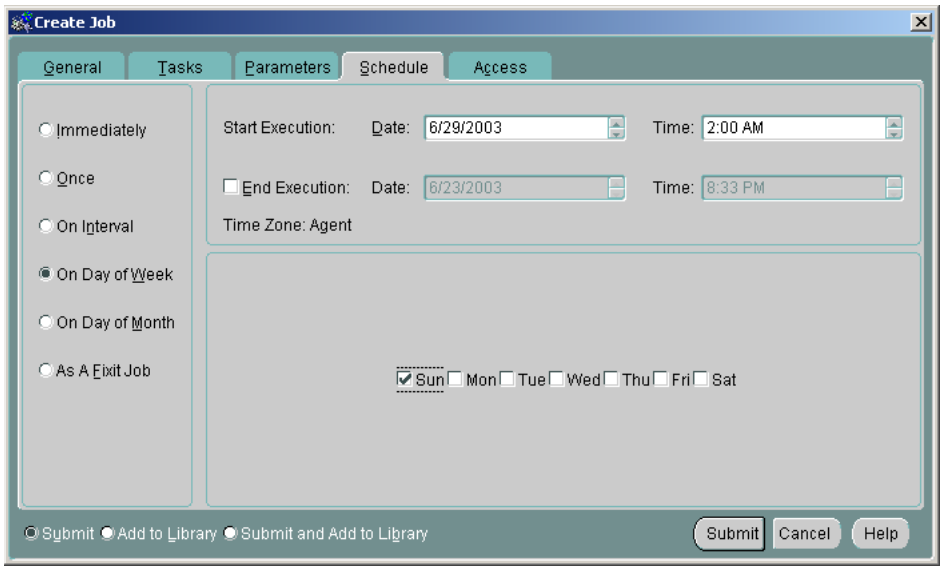
9 In the **Command** box, enter the following command: **/IMS/imssipdb/data/db_schema/backup/export_imsdb1.sh**

10 In the **Arguments** box, enter the following argument format: **<db_type> <name_of_backup> <media_type>** where **db_type** is PRIMARY (or SECONDARY, when within a redundant architecture), **name_of_backup** is the name of the backup file, and **media_type** is DISK or TAPE.

Schedule backup frequency

11 Click the **Schedule** tab.

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



12 Select **On Day of Week**. Next, select the day of the week on which the backup should run.

Note: A backup job should be created for each day of the week.

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

Submit and add the backup job to the library

14 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.

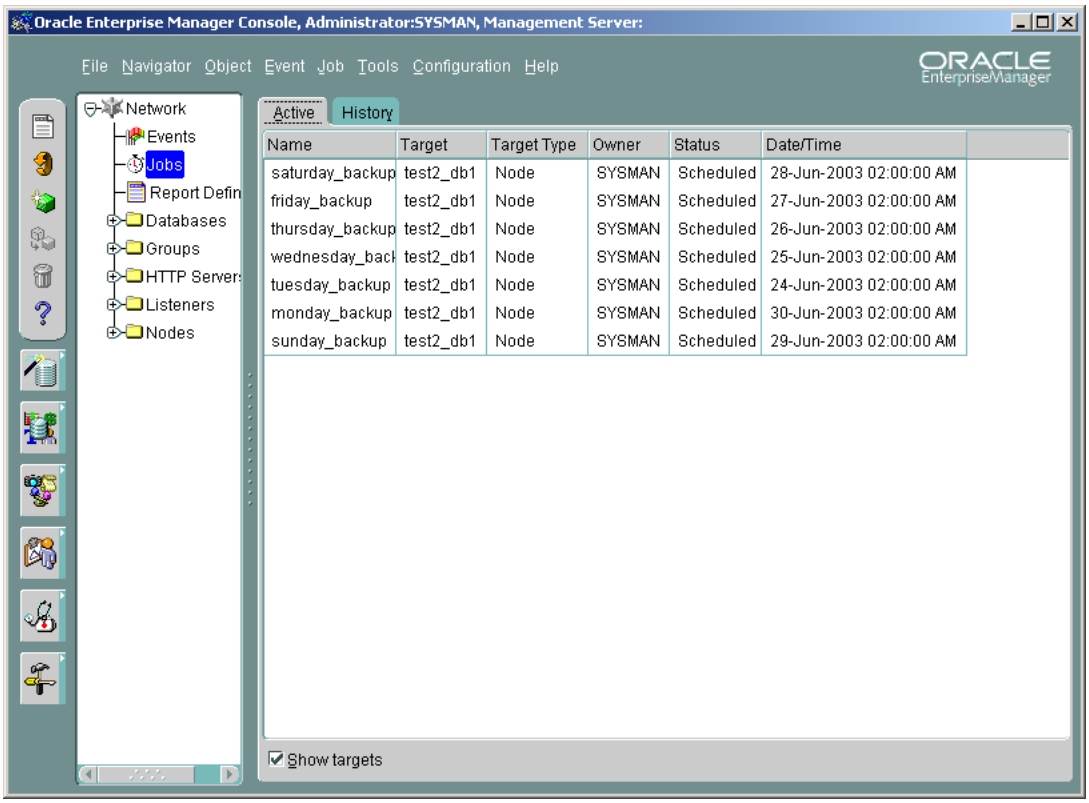
The Create Job dialog box closes and the new backup job appears in the Active > Jobs tab.

Modifying a scheduled Export/Import Oracle database backup job
Use the following procedure to modify scheduled Export/Import backup jobs from the OEM Console:

For instructions on logging in, please refer to Logging in to the OEM Console on page 73.

From the OEM Console

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

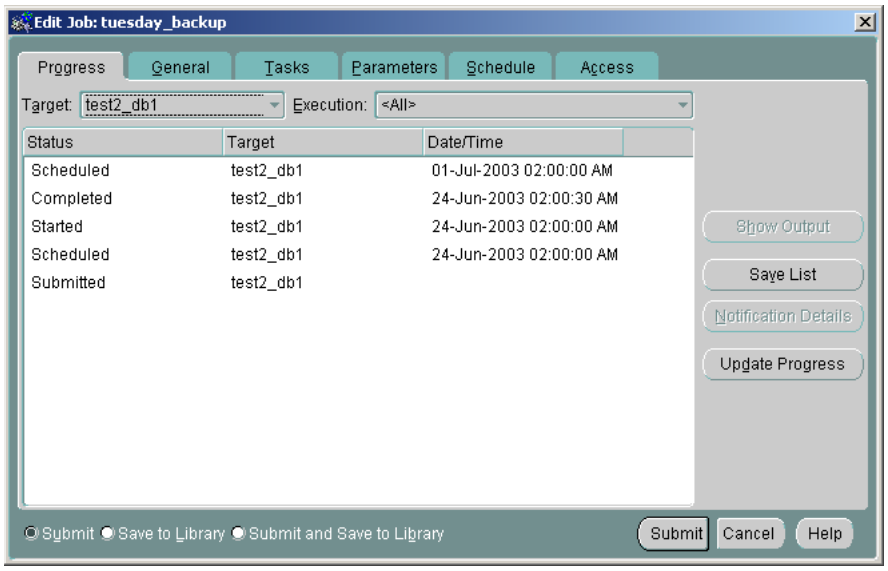


The **Jobs >Active** tab displays the list of active backup jobs that have been scheduled.

2 On the **Active** jobs panel, select the job that to be modified.

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 110.

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.

Oracle database recovery using Export/Import

Database recovery is achieved by restoring a previous backup version of the Oracle database. In a redundant architecture, the Oracle databases would then need to be resynced using the procedure outlined in Resynchronization (only in a redundant architecture) on page 49.

Restoring exported Oracle database backup files

CAUTION

Only trained personnel should perform the following task.

Use the following procedure to restore files created using the Export/Import backup method:

Note 1: Stop all MCS network components that connect to the Oracle database (for example, the Oracle Monitor, Provisioning Module, SIP Application Module, IP Client Manager, Web Client Manager, and Management Module) before performing this procedure. After the procedure is completed, start all MCS network components to return them to their previous state.

Note 2: The approximate import time, when recovering a database, is 100 MegaBytes of data per hour.

On the server hosting the primary database

1 Shut down the primary database as follows:

- **a** Log in as **root**.
- **b** Execute the following commands:

  cd /etc/init.d

  ./dbora stop

2 Set up a clean database as follows:

- **a** Log in as **oracle**.
- **b** Execute the following commands:

  cd /export/home/oracle/bin

  restore_empty_db

3 Start up the primary database as follows:

- **a** Log in as **root**.
- **b** Execute the following commands:

  cd /etc/init.d

  ./dbora start

4 Restore the primary database as follows:

a Log in as **oracle** to the server hosting the primary database.

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.

Note: If restoring the database from disk, the name_of_backup file must be located within the /backup/orabackup directory.

Restoring control files

Use the following procedure to restore control files:

Note: Stop all MCS network components before performing this procedure.

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

On the server containing the damaged files

1 Log in 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 Log in as **oracle** to the server hosting the primary database.

7 Restart the database as follows:

cd /IMS/imssipdb/data/db_schema/util

stop_imsdb abort

start_imsdb

Generating reports

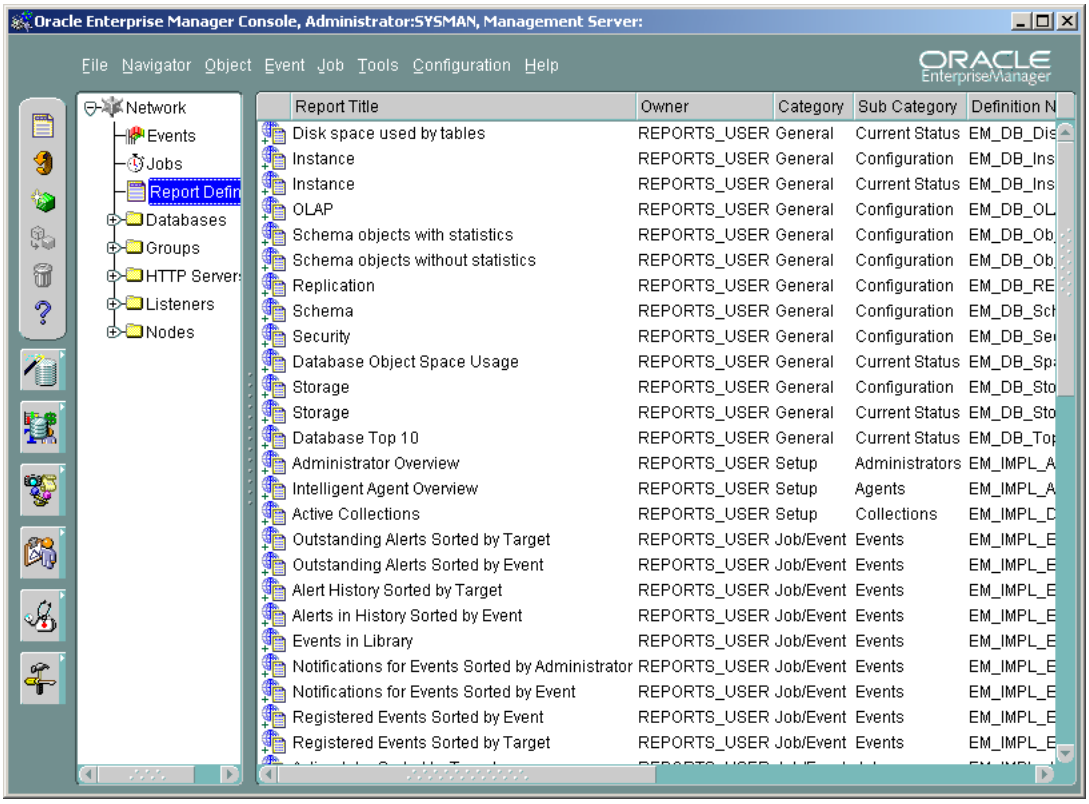
Reports can be generated using the OEM Console in order to provide additional information on the Oracle database. For a list of recommended reports, please refer to Table 32, Recommended database reports, on page 102.

Use the following procedure to generate a report:

From the OEM Console

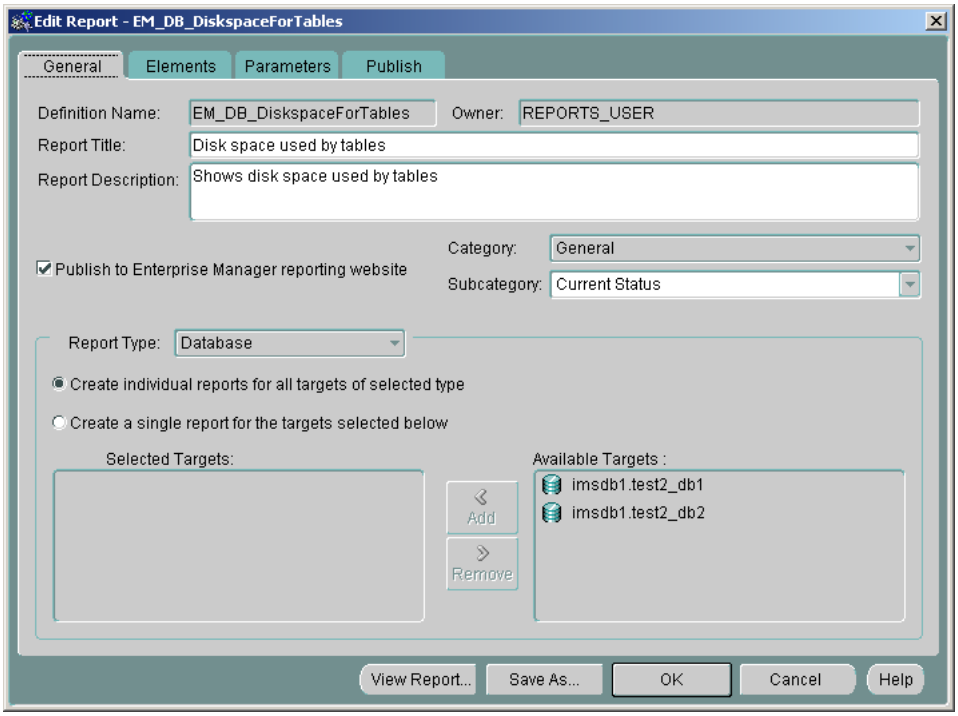
1 From the **Network** tree, select the **Report Definitions** node.

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.

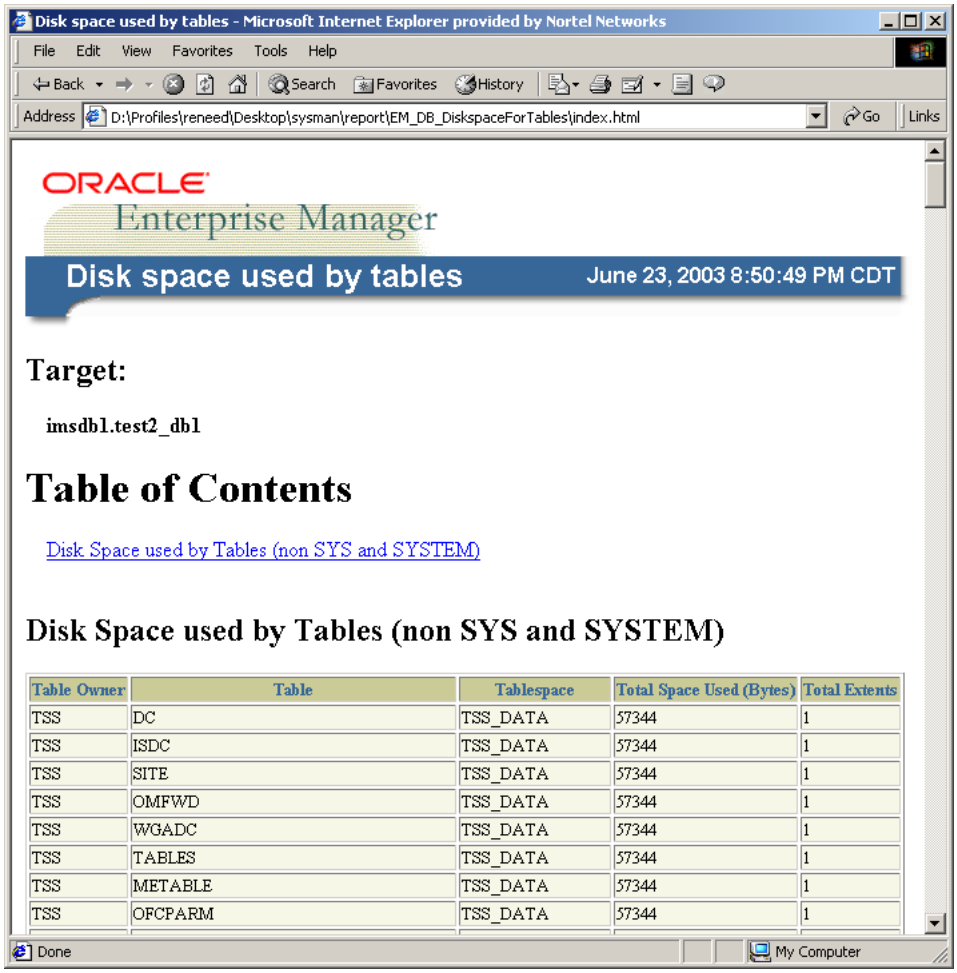


3 Select **Create a Single Report for the Targets Selected Below**.

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.


Disk space used by tables - Microsoft Internet Explorer provided by Nortel Networks
File Edit View Favorites Tools Help
Back Search Favorites History
Address D:\Profiles\reneed\Desktop\sysman\report\EM_DB_DiskspaceForTables\index.html
Go Links
ORACLE
Enterprise Manager
Disk space used by tables
June 23, 2003 8:50:49 PM CDT
Target:
imsdb1.test2_db1
Table of Contents
Disk Space used by Tables (non SYS and SYSTEM)
Disk Space used by Tables (non SYS and SYSTEM)
Table Owner | Table | Tablespace | Total Space Used (Bytes) | Total Extents
TSS | DC | TSS_DATA | 57344 | 1
TSS | ISDC | TSS_DATA | 57344 | 1
TSS | SITE | TSS_DATA | 57344 | 1
TSS | OMFWD | TSS_DATA | 57344 | 1
TSS | WGADC | TSS_DATA | 57344 | 1
TSS | TABLES | TSS_DATA | 57344 | 1
TSS | METABLE | TSS_DATA | 57344 | 1
TSS | OFCPARM | TSS_DATA | 57344 | 1
Done
My Computer

Succession

Carrier Voice over IP

Database Module Basics

Publication number: NN10368-111
Product release: (I)SN07
Document version: Standard 02.02
Date: December 2004

NORTEL NETWORKS™