Oracle® Database

Readme

11*g* Release 1 (11.1)

B28280-02

August 2007

Purpose of this Readme

This Readme file is relevant only to the delivered Oracle Database 11*g* Release 1 (11.1) product and its integral parts, such as SQL, PL/SQL, the Oracle Call Interface (OCI), SQL*Loader, Import/Export utilities, and so on.

This Readme documents differences between the server and its integral parts and its documented functionality, as well as known problems and workarounds.

For additions and corrections to the server documentation set, refer to the Oracle Database Documentation Addendum, which is available on the product CD. A complete list of open known bugs is also available on the product CD.

Operating system releases, such as UNIX and Windows, often provide readme documents specific to that operating system. Additional Readme files may also exist. This Readme file is provided in lieu of system bulletins or similar publications.

Contents

ORACLE®

1 Compatibility, Upgrading, Downgrading and Installation

Note the following items for compatibility, upgrading, downgrading, and installation.

1.1 New Time Zone File Version

A new time zone file, version 4, is used with Oracle Database 11*g* Release 1 (11.1). If you have not already moved to time zone file version 4, then you must apply patch 4689959 to your existing databases prior to upgrading.

You can use SELECT VERSION FROM V$TIMEZONE_FILE to identify the time zone file version used by your 10*g* databases. The Pre-Upgrade Information Tool (utlu111i.sql and its counterpart used by the Database Upgrade Assistant) provides a warning if the time zone file version is not version 4, and it also updates a table in the database with the actual time zone version in use. Later, when the upgrade script is run (for both manual and DBUA upgrades), the upgrade script will terminate without running the upgrade if the stored time zone file value is not the same as the time zone file version the Oracle Database 11*g* server is using.

If your existing databases are using a time zone file version greater than 4, then you will need to apply the appropriate patch to the Oracle Database 11*g* Oracle Home prior to upgrading any databases so that the 11*g* server will be using the same time zone file version as your existing databases.

For additional information about time zones, see Section 35, "Time Zones".

1.2 Oracle Universal Installer runInstaller Error

When the following `runInstaller` command is invoked, the `"Error in execution of Additional utility tool"` error is returned:

```
./runInstaller -printdiskusage -printmemory -printtime
```

Along with the error, you will see `Help`, `Retry`, `Continue`, and `Cancel` buttons. Click on `Continue` and the installation will proceed (reference Bug 6271506).

1.3 Standard Edition Starter Database Upgrade

When the Standard Edition (SE) starter database is upgraded, the following components cannot be upgraded by the SE server because they require options that are not installed in the Standard Edition:

- OLAP Catalog
- OLAP Analytic Workspace
- Oracle OLAP API

After the upgrade, these components will have a `STATUS` value of `'OPTION OFF'` in the `DBA_REGISTRY` view, and there will be some invalid objects in the associated component schemas. The Database Upgrade Assistant (DBUA) will show unsuccessful upgrades for these components (reference Bug 6111079).

1.4 Tablespace and Flash Recovery Area Sizing

The Oracle Database 11*g* Pre-Upgrade Information Utility (`utlu111i.sql`) estimates the additional space required in the `SYSTEM` tablespace and in any tablespaces associated with the components that are in the database (for example, SYSAUX, DRSYS). For a manual upgrade, be sure to run this utility on your existing database prior to upgrading.

The tablespace size estimates may be too small, especially if XDB is installed in your database. However, to avoid potential space problems during either a manual upgrade or an upgrade using the Database Upgrade Assistant (DBUA), you can set one data file for each tablespace to `AUTOEXTEND ON MAXSIZE UNLIMITED` for the duration of the upgrade.

If you are using file systems for data file storage, be sure there is adequate space in the file systems for tablespace growth during the upgrade.

If you are using a Flash Recovery Area, check that the size available is sufficient for the redo generated during the upgrade. If the size is inadequate, an `ORA-19815` error will be written to the alert log, and the upgrade will halt until additional space is made available.

1.5 Setting Memory Target at Instance Startup on Linux

Starting with Oracle Database 11*g* Release 1 (11.1), Oracle provides the option of automatically managing SGA and PGA with a combined `MEMORY_TARGET` parameter without having to set `SGA_TARGET` and `PGA_AGGREGATE_TARGET` explicitly. This is supported on Linux, Windows, Solaris, HPUX and AIX.

If you see the `ORA-00845` error reported on Linux machines at Oracle instance startup when using the `MEMORY_TARGET` parameter, check the size of `/dev/shm`. If `/dev/shm` is not configured, mount it sized to be at least `MEMORY_TARGET`. If `/dev/shm` is configured but the amount of available space reported (through `df -k /dev/shm`) is less than `MEMORY_TARGET`, free up the space or mount a larger `/dev/shm` to satisfy the `MEMORY_TARGET` size. Note that if you set the `MEMORY_MAX_TARGET` parameter greater than `MEMORY_TARGET`, ensure that `/dev/shm` is sized to be at least `MEMORY_MAX_TARGET`.

1.5.1 Memory Target for Oracle Database Instances

Running Database Configuration Assistant (DBCA) defaults to this Automatic Memory Management option. In the case of upgrade or manual database creation, `MEMORY_TARGET` can be specified in the initialization parameter files.

1.5.2 Memory Target for ASM Instances

Automatic Storage Management (ASM) instances default to Automatic Memory Management of the SGA and PGA starting with 11.1.0.6, even if the `MEMORY_TARGET` parameter is not explicitly set. To disable Automatic Memory Management for ASM, you must explicitly set `MEMORY_TARGET` to `0`. DBCA does not allow `MEMORY_TARGET` to be set for ASM instances. To disable Automatic Memory Management, `MEMORY_TARGET` must be manually set to `0`.

1.6 Upgrading Databases with *inter*Media, Spatial, or XDK for Java

Oracle *inter*Media (now called Oracle Multimedia), Oracle Spatial, and Oracle XDK for Java use the Oracle XML DB. If any of these components are installed with the database, Oracle XML DB is automatically installed to support them.

1.7 Compatibility with Oracle9*i* Release 2 Database

Connecting Oracle Database 11*g* Release 1 (11.1) client or server to Oracle9*i* Database release (9.2.0.4 and above) is supported. Similarly, connecting Oracle9*i* client (release 9.2.0.4 and above) to Oracle Database 11*g* Release 1 (11.1) is supported.

1.8 Enabling Automated Backups

While installing Oracle Database, the Specify Backup and Recovery Options screen may appear truncated if your system does not have the required fonts installed. If your system has only fixed-width fonts, you may not be able to fully specify the required information in the Backup Job Credentials area of the screen. To work around this issue, do not select **Enable Automated Backups** on this screen. After the installation is complete, use Oracle Enterprise Manager 11*g* Database Control to enable automated backups.

1.9 Upgrading a Database With SQL Access Advisor Tasks

Due to internal structural changes to the SQL Access Advisor repository, a database upgrade resets all existing SQL Access Advisor tasks to their initial state. This effectively deletes all recommendation information for tasks that have successfully executed prior to upgrade.

After upgrade, the recommendation information can be restored by reexecuting the existing SQL Access Advisor tasks.

1.10 Downgrade to Release 10.2.0.3

If you anticipate downgrading back to release 10.2.0.3, you need to apply the patch for Bug 4309607 to the 10.2.0.3 Oracle Home prior to running `catrelod.sql`. This patch is not needed for later 10.2.0.*x* patch releases.

1.11 Oracle Clusterware Upgrade

In Oracle Database 11*g* Release 1 (11.1), there is a new prerequisite check during the Oracle Clusterware upgrade cycle. On failure of this prerequisite check, the *Oracle Database Upgrade Guide* documents the following:

> When upgrading clusterware from Oracle Clusterware 10*g* Release 2 (10.2) to Oracle Clusterware 11*g* Release 1 (11.1), you must first apply the patchset version 10.2.0.3.0 or later to your existing clusterware before it can be upgraded.

Apart from this proposed solution, there is an alternative solution. You can choose to upgrade all nodes of the cluster simultaneously in a nonrolling manner. If you choose this solution, the 10.2.0.3.0 patchset requirement is void.

1.12 Resource Not Found Exception With Oracle BI Publisher Installer

You may see the following errors in the `installActions.log` file and in the command window used to launch Oracle BI Publisher Installer (reference Bug 6243068):

```
oracle.apps.xdo.servlet.resources.ResourceNotFoundException:
%s_Reports_Path%/Admin/Security/principals.xml
```

These errors can be safely ignored.

2 Features Not Available or Restricted in This Release

The following is a list of components that will not be available or are restricted in Oracle Database 11*g* Release 1 (11.1):

- Edition-based redefinition is not available in Oracle Database 11*g* Release 1 (11.1). You cannot create an edition, an editioning view, or a crossedition trigger; nor can you use the `ENABLE EDITIONS` clause in the `CREATE USER` and `ALTER USER` commands. As a consequence, other related functionality (for example, the `ALTER SESSION SET EDITION` statement or the new overload of `DBMS_Sql.Parse()` that lets you specify an edition or a crossedition trigger) becomes uninteresting and attempting to use it will cause a semantic error.

- Oracle Workflow is not shipping with Oracle Database 11*g* Release 1 (11.1).

- See Section 9.1 for globalization restrictions within Oracle Secure Backup.

- See Section 26 for current limitations with the Oracle XML Developer's kit.

- Database native web services used in an Oracle RAC configuration are not supported.

- The original Export utility is no longer supported for general use. The original Import utility is still supported. However, Data Pump Export and Data Pump Import are the recommended and fully supported utilities for exporting and importing data in Oracle Database 11*g* Release 1 (11.1).

- In this release, passwords *are* case sensitive by default. This behavior is different from previous releases.

- Network File System (NFS) support in Oracle XML DB is not supported.

- Downgrade from Oracle Database 11*g* Release 1 (11.1) to release 10.2.0.3 is not supported with Oracle Database Vault.

- Oracle Clusterware patching procedure is not supported from Enterprise Manager Database Control for Oracle Database 11*g* Release 1 (11.1).

3 Default Behavior Changes

This section describes some of the differences in behavior between Oracle Database 11*g* Release 1 (11.1) and previous releases. The majority of the information about upgrading and downgrading is already included in the *Oracle Database Upgrade Guide*.

3.1 Core Dump Location for OCI Applications

On UNIX systems, when an application program crashes due to an unhandled signal, such as segmentation fault, a core file is normally generated. The system default for that core file name is core located in the current directory in which the application is running. Applications using the Oracle Call Interface (OCI), however, may instead create core files in a special diagnostic directory. Please see the *Oracle Call Interface Programmer's Guide* for details.

3.2 Changes in the Location of Database Diagnostic Files

All trace files, core files, and the alert log will be stored in the Automatic Diagnostic Repository which is a directory structure rooted in the location specified by the DIAGNOSTIC_DEST initialization parameter. The parameters BACKGROUND_DUMP_DEST and USER_DUMP_DEST are now ignored.

3.3 Offset for CLOB and NCLOB APIs

Starting with Oracle Database 10*g* Release 1 (10.1), APIs that write to a CLOB or NCLOB cause error ORA-22831 when the offset specified for the beginning of the write is not on a character boundary of the existing LOB data.

LOB APIs use UCS2 codepoint semantics for the amount and offset parameters on CLOBs or NCLOBs when the database default or national character set is multibyte. The specified offset is not on a character boundary if it points to the low (second) surrogate of a surrogate pair. In such situations, error ORA-22831 occurs and the data is not written. This prevents corrupting the character in the target LOB.

Contact Oracle Support Services to configure the database so that it does not return `ORA-22831`.

3.4 LOG_ARCHIVE_DEST_*n* Parameter

The `LOG_ARCHIVE_DEST_n` parameter can now be used to specify a local archiving destination on a database instance running Oracle Standard Edition. Previously, this parameter could only be specified on a database instance running Oracle Enterprise Edition.

3.5 SHARED_POOL_SIZE Parameter

Prior to Oracle Database 10*g* Release 1 (10.1), the amount of shared pool memory allocated by previous Oracle Database releases was equal to the sum of the value of the `SHARED_POOL_SIZE` initialization parameter and the internal SGA overhead computed during instance startup. This overhead was based on the values of several other initialization parameters. As an example, if the `SHARED_POOL_SIZE` parameter is 64m and the internal SGA overhead is 12m, the real size of shared pool in the SGA would be 76m, although the value of the `SHARED_POOL_SIZE` parameter would still be displayed as 64m.

In Oracle Database 10*g* Release 1 (10.1), the size of internal SGA overhead was included in the value of `SHARED_POOL_SIZE` parameter; the shared pool memory allocated at startup was exactly the value of `SHARED_POOL_SIZE`. Therefore, this parameter had to be set such that it included both the internal SGA overhead and the desired effective value of the shared pool size. Assuming that the internal SGA overhead remained unchanged, the effective available value of shared pool after startup would be 12m less than the value of the `SHARED_POOL_SIZE` parameter, or 52m. To maintain 64m for the effective value of shared pool memory, set the parameter to 76m.

Migration utilities for this release recommend new values for `SHARED_POOL_SIZE` based on the value of internal SGA overheads in the pre-upgrade environment, which you can determine by running the following query before upgrading to Oracle Database 11*g* Release 1 (11.1):

```
SQL> SELECT SUM(BYTES) FROM v$sgastat WHERE pool = 'shared pool';
```

In Oracle Database 11*g* Release 1 (11.1) the exact value of internal SGA overhead, or Startup overhead in Shared Pool, is listed in the new `v$sgainfo` view.

In the *manual* SGA mode, values of `SHARED_POOL_SIZE` that are too small to accommodate the internal SGA overhead result in an `ORA-00371` error during startup. This generated error message includes a suggested value for the `SHARED_POOL_SIZE` parameter.

If you are using *automatic* shared memory management, the size of the shared pool is tuned automatically, and the `ORA-00371` error is never generated.

3.6 SHARED_SERVERS Parameter

When the initialization parameter `SHARED_SERVERS` is dynamically changed to `0`, no new clients can connect in shared mode, but existing shared server connections can continue to operate. Prior to Oracle Database 10*g*, existing shared server connections would hang in this situation.

3.7 Default Storage of Varrays

In Oracle Database 11*g* Release 1 (11.1), the default storage of varrays has changed from index-organized tables (IOTs) to heap-organized tables. The benefit is improved performance obtained by heap partitioning for large documents. However, for small documents, performance is better using IOTs.

3.8 JOB_QUEUE_PROCESSES Parameter

Beginning with Oracle Database 11*g* Release 1 (11.1), `JOB_QUEUE_PROCESSES` has changed from a basic to a non-basic initialization parameter. Most databases should be required to have only basic parameters set to run properly and efficiently.

In earlier Oracle Database releases, `DBMS_JOB` and `DBMS_SCHEDULER` shared the same job coordinator, and its behavior was controlled by the `JOB_QUEUE_PROCESSES` parameter. Now `DBMS_JOB` and `DBMS_SCHEDULER` work without setting this initialization parameter. You can still set it if you want, but you are no longer required to set it.

The range of supported values for `JOB_QUEUE_PROCESSES` is still `0-1000`. However, the default value has been changed from 0 to 1000. If it is set to `0`, then `DBMS_SCHEDULER` jobs run, and `DBMS_JOB` jobs do not run. The number of slave processes created for DBMS_SCHEDULER jobs is autotuned based on the load of the computer.

If `JOB_QUEUE_PROCESSES` is set to a value in the range of `1-1000`, then both DBMS_JOB jobs and `DBMS_SCHEDULER` jobs run, and the number of slave processes created for these jobs is autotuned with an additional restriction that the total number of slave processes is capped at the value of JOB_QUEUE_PROCESSES.

4 Configuration Assistants

Note the following when working with NET Configuration Assistant (NETCA).

4.1 NET Configuration Assistant (NETCA)

During creation of a new Oracle RAC 11*g* (11.1) database or upgrading of an Oracle RAC 10*g* database, NETCA may be run to migrate listeners from the 10*g* Oracle Home to 11.1 Oracle Home. If for some reason migration fails on remote nodes, database creation or upgrade succeeds. However, listeners may not have been configured on the remote nodes where failure occurred. Perform one of the following workarounds to resolve this:

- Resolve the problem condition and rerun NETCA `migrate` on any failed node as:

  ```
  netca /migrate /nodeinfo comma_separated_list_of_remaining_nodes
  ```

- Run NETCA in standalone mode to delete any existing listeners on the failed nodes and re-create 11.1 listeners.

5 Oracle Enterprise Manager Database Control

The following sections describe information for Database Control in Oracle Database 11*g* Release 1 (11.1).

5.1 Reorganize Objects

The following applies to Reorganize Objects:

- The database can be adversely affected if metadata changes occur between the time the reorganization script is generated and the time it is executed.

- The database can be adversely affected if an offline reorganization is attempted while DDL is in progress against the tables being reorganized.

- Before using the Reorganize Objects wizard or the Make Tablespace Locally Managed wizard in Enterprise Manager, Oracle recommends that you back up your database.

Error in Impact Report

When reorganizing a tablespace with Enterprise Manager in a 10*g* or 11*g* database, you may encounter the following error message in the Impact Report:

```
This tablespace contains recycle-bin segments from tables that have been
dropped. It cannot be reorganized. Use the PURGE TABLESPACE command to remove
the recycle-bin segments from the tablespace and re-try the reorganization.
```

The `PURGE TABLESPACE` command only removes recycle-bin segments belonging to the currently connected user. Therefore, it may not remove all the recycle-bin segments in the tablespace. You can determine which users have recycle-bin segments in a target tablespace using the following query:

```
SELECT DISTINCT owner FROM dba_recyclebin WHERE ts_name = "TARGET_TS";
```

You can then use the following command to purge the segments for each of the users:

```
PURGE TABLESPACE target_ts USER scott;
```

An alternative is to use the following commend:

```
PURGE DBA_RECYCLEBIN;
```

The `PURGE DBA_RECYCLEBIN` command can be used only if you have `SYSDBA` system privileges. It removes all objects from the recycle bin, regardless of user.

5.2 Editing Multiple Objects

Enterprise Manager only supports having one browser window open for editing an object. For example, Enterprise Manager only supports editing one tablespace at a time. Note, if a window is read-only, you may have multiple browser windows open.

5.3 Database Performance Page Shows Grey Area Instead of Graphs in Internet Explorer

Sometimes in Internet Explorer, the SVG graphs on the Database Performance page do not render properly. Instead, the page displays a large grey area with no

graphs at all. This problem can occur for different reasons. Try the following workarounds:

- Change a setting in your Internet Explorer browser as follows:

    1. Click Tools, click Internet Options, and click the Advanced tab

    2. Scroll down to Security and uncheck "Do Not Save Encrypted Pages to Disk."

- If there is a lot of contention for the CPU on the machine hosting the Oracle Management Service (OMS), try increasing the browser time-out interval from 1 minute (the default) to 5 minutes. Microsoft Knowledge Base article no. 813827 provides instructions on how to do this (http://support.microsoft.com/default.aspx?kbid=813827).

5.4 Requirements for Proxy Settings for XDB

The following are requirements for XDB proxy settings:

- For an XDB Resource to be created using a URL behind the firewall, the proxy in `emoms.properties` needs to be set.

- When registering an XML Schema based on a URL, the URL is interpreted by the database itself, in which case, the database proxy might need to be set.

> **Note:** If the proxy settings cannot be changed, a valid workaround would be to save these files locally in the client machine and then use the "Local File" option to create a resource or register a schema.

5.5 Password Fields Ignored When Granting Enterprise Manager Administration Privileges to Existing Database Users

The page in Oracle Enterprise Manager that enables you to create new Enterprise Manager Administrators enables you to either assign Enterprise Manager administration privileges to an existing database user or to create a new Enterprise Manager administrative user, which also creates a database user account for that user. The `Password` and `Confirm Password` fields on the Create Administrator page behave differently depending on whether you are creating a new user or assigning Enterprise Manager administration privileges to an existing database user. If you are creating a new administrator (and thus a new database user), you are assigning a database password for that user. If you are assigning Enterprise Manager administrative privileges to an existing user, whatever text you enter in the password fields is ignored, and the user's database password is not changed.

6 Database Security

Note the following changes in Database Security.

6.1 Password Change Prevented on an Expired Account

You are prevented from using Oracle Database 10.1.*x* and Oracle Database 10.2.*x* clients to connect to an Oracle Database 11g Release 1 (11.1) server using an expired password to perform a password change (reference Bug 6277160).

To work around this problem, request that someone with the `ALTER USER` privilege reset the password for the expired account. Or, use an Oracle Database 11g Release 1 (11.1) database client to perform the password change.

6.2 Changes in Default Security Settings

Java class `oracle.security rdbms.server.AppCtx` will be deprecated in future Oracle Database releases.

6.3 Enterprise User Security

The following apply to Enterprise User Security:

■ Databases with different methods of authenticating to Oracle Internet Directory cannot share the same `ldap.ora` file.

   If these databases use the same `$ORACLE_HOME`, each database should have a separate `TNS_ADMIN` environment variable that points to its own `ldap.ora` file (reference Bug 3327626).

7 Encryption and Integrity

Note the following changes in the areas of encryption and integrity.

7.1 Data Integrity

Oracle recommends the use of SHA-1 for data integrity for protected communication between clients and servers. Using MD5 in cipher suites that affect short-timed transactions such as during SSL/TLS authentication or using keyed MD5 for one-way hash stores and using MD5 in SSL/TLS protocols have not been identified as being vulnerable at this time.

7.2 Encrypted Tablespaces

You cannot encrypt an existing tablespace with an `ALTER TABLESPACE` statement. However, you can use Data Pump or SQL statements such as `CREATE TABLE AS SELECT` or `ALTER TABLE MOVE` to move existing table data into an encrypted tablespace.

When recovering a database with encrypted tablespaces (for example, after a `SHUTDOWN ABORT` or a catastrophic error that brings down the database instance), you must open the wallet after database mount and before database open so the recovery process can decrypt data blocks and redo.

8 Java and Web Services

Note the following items when working with Java.

8.1 Oracle JVM

Oracle Database 11*g* Release 1 (11.1) includes a fully functional Java Virtual Machine (JVM), as well as the Java class libraries for Sun's Java Development Kit (JDK) 5.0. When combined with Oracle's JDBC and SQLJ, this release provides an

enterprise class platform, Oracle JVM, for developing and deploying server-based Java applications.

8.1.1 What's New in This Release

There are a number of changes and new features for the Oracle Database 11*g* Release 1 (11.1).

8.1.1.1 Oracle JVM Compatibility With JDK 5.0 The system classes in Oracle JVM are upgraded from JDK 1.4 level to JDK 5.0. For additional information, see http://java.sun.com/j2se/1.5.0/docs/relnotes/features.html.

8.1.1.2 Oracle JVM Utilities Enhancements The utilities enhancements include:

- URL support in loadjava
- List-based operation with `dropjava`
- Class closure tool
- `ojvmjava` enhancements

8.1.1.3 Usability Enhancements The following apply:

- JDK-like command-line interface
- Database-resident JAR support
- Sharing of metadata for user classloaded classes
- Two-tier duration for Java session state
- Direct and immediate termination of Java sessions
- Redirection output on the server
- Support for JMX interface

8.1.1.4 Just-In-Time (JIT) Compiler The JIT compiler complies Java bytecode on-the-fly resulting in hugh enhancement of the of Java execution time (as compared with interpreted mode). The JIT stores the compiled binaries avoiding recompilation. It is enabled by default and can be disabled using the `java_jit_enabled=false` initialization parameter. To reenable, use `java_jit_enabled=true`.

8.1.2 Configuration

The *Oracle Database Java Developer's Guide* provides details for installing and configuring a Java-enabled database. The use of Oracle JVM requires increasing `shared_pool` and `java_pool` limits.

The primary initialization parameters that can affect Java usage and performance are `shared_pool_size` and `java_pool_size`.

8.1.2.1 shared_pool Memory The `shared_pool` memory is consumed mainly during Java initialization in the database (for example, `initjvm.sql`), loadjava, Java source compilation, and call-specifications processing. How much increase is required depends on usage but at least `shared_pool_size = 96M` is recommended.

8.1.2.2 java_pool_size Memory The `java_pool_size` is used mainly for in-memory representation of Java method and class definitions, static Java states that are migrated to session space at end-of-call in shared server mode. How much increase is required depends on usage but at least `java_pool_size = 50M` is recommended.

8.1.3 JDK 5.0 Compatibility

This release has been thoroughly tested with Sun's Java Compatibility Kit for JDK 5.0. Oracle is committed to Oracle JVM keeping pace with Java and other internet standards.

8.1.4 Message Order Incorrect

If you use Oracle Java Messaging Service (OJMS) or Messaging Gateway, the message order can be incorrect when you use the Java Messaging Service (JMS) selector.

One of the following will correct this behavior:

- If you use Oracle Java Messaging Service, you are required to grant the `ALTER SESSION` privilege to the OJMS users. However, if you use Messaging Gateway, you are required to grant `ALTER SESSION` privilege to the `MGW_AGENT_ROLE`.

- You can also set the `oracle.jms.orderWithSelector` Java system property to `false` when using OJMS. When this property is set to `false`, OJMS does not require the ALTER SESSION privilege for its users. However, in this case, the message order can sometimes be wrong when the Java Message Service (JMS) selector is used.

8.2 JDBC

In this release, key JDBC features include support of the latest Java/JDBC standards (such as JDK 6 and JDBC 4.0) and the exposure of new Oracle Database 11*g* Release 1 (11.1) features to Java Developers (such as new SQL types, Streams/AQ, and Diagnosability).

For more details, see:

```
$ORACLE_HOME/jdbc/Readme.txt
```

8.2.1 Support for Java Standards: JDK 6.0 and JDBC 4.0

Support for Java standards include:

- Enhancements to Statement, ResultSet, and Wrapper Pattern

- New SQLException framework

- Enhancements to `BLOB` and `CLOB`

- New standard data types (`java.sql.*`)

8.2.2 Support for New Oracle Database Features

New feature support includes:

- New data types (`AnyType` and `AnyData`)

- Advanced security option for JDBC-thin (Kerbers, Radius, SSL authentication, SHA1 checksum and AES encryption)

- Support for Database Change Notification for cache invalidation

8.2.3 New Performance, Scalability and Manageability Features

New performance, scalability and manageability features include:

- Streams AQ integration and new native AQ protocol for JDBC-thin

- Prefetch in first round trip for JDBC-thin

- Support for JMX interface

- Database startup and shutdown

- Support for OCI client result cache

8.3 Web Services

As an alternative to Oracle Net, Oracle Database Web services provides nonconnected access to the database through standard Web services mechanisms. These include XML, SOAP, and WSDL, and can turn the database into a Web services provider. Similarly, the database itself can act as a Web service consumer and invoke external Web services. Important features of Web services include:

- A JAX-RPC based SOAP Client library supports invocation of external Web services from within the database, and applies the power of SQL to the results.

- **Web Services Call-In:** Deploying a JPublisher-generated Java class against Oracle Application Server 10*g* enables you to invoke database operations like Java and PL/SQL procedures and packages, SQL queries, and DML operations.

- **Web Services Call-Out:** Deploying a JPublisher-generated Web services client from a WSDL and its PL/SQL wrapper supports invocation of external Web services from within the database.

9 Media Management Software

For environments that consist of a single server, Oracle offers Oracle Secure Backup Express to back up your Oracle Database and other critical Oracle infrastructure to tape. Oracle Secure Backup is fully integrated with Recovery Manager (RMAN) to provide data protection services. For larger environments, Oracle Secure Backup is available as a separate licensable product to back up many database servers and file systems to tape. Oracle Secure Backup release 10.1.0.3.0 is shipping with this Oracle Database 11*g* Release 1 (11.1). For more information on Oracle Secure Backup, refer to

http://www.otn.oracle.com/products/secure-backup/index.html

9.1 Globalization Restrictions Within Oracle Secure Backup

The following globalization restrictions apply to Oracle Secure Backup:

- The Oracle Secure Backup Web Tool and command line interface are English only, and are not globalized. All messages and documentation are in English.

- Oracle Secure Backup does not support file names or RMAN Backup names that are encoded in character sets that do not support null byte termination, such as Unicode UTF-16. Note this restriction affects file names, not backup

contents. Oracle Secure Backup can back up Oracle databases in any character set.

10 Oracle Application Express

With release 2.2, Oracle HTML DB has been renamed to Oracle Application Express. To learn more about Oracle Application Express release 3.0, refer to *Oracle Database Application Express Release Notes* and *Oracle Database Installation Guide.*

10.1 Checking for the Most Current Release

Oracle Application Express is released more frequently than the Oracle Database. To view additional information about the most current release, refer to

http://www.otn.oracle.com/products/database/application_express/

10.2 Configuring Oracle HTTP Server

When configuring Oracle HTTP Server for Application Express in a new installation, the database user APEX_PUBLIC_USER must be an unlocked account. To unlock the account for database user APEX_PUBLIC_USER, execute the following:

1. Start SQL*Plus and connect as SYS to the database where Oracle Application Express is installed. For example:

    ```
    $ $ORACLE_HOME/bin/sqlplus
    SQL> CONNECT SYS as SYSDBA
    Enter password: SYS_password
    ```

2. Run the following command:

    ```
    SQL> ALTER USER APEX_PUBLIC_USER ACCOUNT UNLOCK
    ```

10.3 Database Compatible Parameter and Enabling Network Services

In order to run the examples in the Application Express Post-Installation tasks in the section titled "Enabling Network Services in Oracle Database 11*g*" in the *Oracle Database Installation Guide*, the COMPATIBLE initialization parameter of the database must be set to at least 11.1.0.0.0. By default, an 11*g* database will already have the parameter set properly, but a database upgraded to 11*g* from a prior version may not.

Refer to the section titled "Creating and Configuring an Oracle Database" in the *Oracle Database Administrator's Guide* for information about changing database initialization parameters.

11 Oracle Configuration Manager

Note the following for Oracle Configuration Manager.

11.1 Unable to Enable and Register Oracle Configuration Manager Through Oracle Installer for Selected Countries

The installation of Oracle Database 11*g* Release 1 (11.1) does not allow for the selection of any of the following countries when enabling the Oracle Configuration Manager (reference Bug 6202838):

Korea, Democratic People's Republic Of
Korea, Republic Of
Moldova
Russia
Tanzania
Holy See (Vatican City State)
Yugoslavia

The workaround is to not enable the Oracle Configuration Manager during the OUI installation but, afterwards, configure it using the command-line interface using the following command:

```
$ORACLE_HOME/ccr/bin/setupCCR csi metalink_username country_code
```

Where:

- *csi* is the Oracle-issued Customer Support Identifier

- *metalink_username* is the Oracle MetaLink User account Username

- *country_code* is the ISO-3166 two character counterpart for the country. The two character country codes are:

    - KP = Korea, Democratic People's Republic Of

    - KR = Korea, Republic Of

    - MD = Moldova

    - RU = Russia

    - TZ = Tanzania

    - VA = Holy See (Vatican City State)

    - YU = Yugoslavia

For additional help on invoking setupCCR, refer to *Oracle Configuration Manager Installation and Administration Guide* or the online help at:

```
$ORACLE_HOME/ccr/bin/setupCCR -h
```

11.2 CRON Configuration Issue

If you are denied access to CRON, the configuration of Oracle Configuration Manager fails with the following error:

```
$ ORACLE_HOME/ccr/bin/setupCCR
** Installing base package **
Deploying core - Version 10.2.5.0.0
Error encountered in package deployment.
```

After the installation is complete, set the environment variable CCR_DISABLE_ CRON_ENTRY to TRUE and try the configuration of Oracle Configuration Manager again using the following command:

```
$ ORACLE_HOME/ccr/bin/setupCCR
```

12 Oracle Data Guard

Note the following when working with Oracle Data Guard.

12.1 Real-Time Query

A physical standby database can be open for read-only access while Redo Apply is active. This capability, which is new in 11*g*, is called Real-Time Query.

A physical standby database instance cannot be opened if Redo Apply is active on a mounted instance. If Redo Apply is active on a mounted instance, use the following SQL statements to stop Redo Apply, open the standby instance read-only, and restart Redo Apply.

If the physical standby database is being managed using SQL*Plus, use:

```
SQL> ALTER DATABASE RECOVER MANAGED STANDBY DATABASE CANCEL;
SQL> ALTER DATABASE OPEN;
SQL> ALTER DATABASE RECOVER MANAGED STANDBY DATABASE USING
        CURRENT LOGFILE DISCONNECT;
```

If the physical standby database is being managed by the Data Guard broker's command-line interface (DGMGRL), use:

```
DGMGRL> EDIT DATABASE standby_db_unique_name SET STATE APPLY-OFF;
SQL> ALTER DATABASE OPEN;
DGMGRL> EDIT DATABASE standby_db_unique_name SET STATE APPLY-ON;
```

In some cases, a physical standby database will be in an inconsistent state after Redo Apply has been stopped or after the apply instance has crashed. When this happens, an attempt to open the physical standby database will result in an `ORA-16004: backup database requires recovery` error. If this happens, Redo Apply must be restarted and then stopped before trying to open the physical standby database.

12.2 DDL Statements that Use DBLINKS

On logical standby databases, avoid using SQL statements such as `CREATE TABLE tablename AS SELECT * FROM bar@dblink` as they may fail.

When a statement is executed on the logical standby database, it accesses the database link at that time. It is not possible to know if the information on the logical standby database is the same as it was at the time the statement was executed on the primary database. When this happens, use the `DBMS_LOGSTDBY.INSTANTIATE_TABLE` procedure for the table being created, and then restart SQL Apply operations.

12.3 Logical Standby Databases on the Same Node as the Primary Database

If a logical standby database is located on the same computer system as the primary database, it is likely that both Oracle Database instances have access to the same directory structure. There are Oracle Database commands that reuse datafiles. If Oracle Database commands that reuse datafiles are applied on the primary database, the commands may also be applied on the logical standby

database. If that happens while the primary database is shut down, it is possible for the logical standby database to claim the file as part of its database and possibly cause damage to the primary database.

For this reason only, Oracle recommends using the following settings when running the primary and logical standby databases on the same computer system:

```
EXECUTE DBMS_LOGSTDBY.SKIP('ALTER TABLESPACE');
```

12.4 Database Guard Stays On in the New Primary Database if a Prepared Switchover Operation Detects a Network Outage

If a logical standby database performs a switchover to the primary database role running in maximum protection mode, and the LGWR process encounters an error with a destination, LGWR reevaluates all destinations to ensure at least one of them is working properly.

If the LGWR process does not find a destination to which it can successfully write the standby redo log file, and if it does not contain any missing log files or gaps, then the primary instance shuts down. Although the switchover completes successfully, the database guard remains enabled to prevent data divergence.

The solution, which appears in the alert log for the database instance, is to:

- Start the database in a lower protection mode, such as maximum performance.

- Manually disable the database guard by issuing the ALTER DATABASE GUARD NONE command.

12.5 SQL Apply Stops Making Progress While Applying Changes to a Table with XMLIndex in ASYNC Mode

SQL Apply processes may block each other while trying to apply updates from two or more apply processes to a table that has an XMLIndex in ASYNC mode with SYNC ON COMMIT specified. This mode is specified with the ASYNC (SYNC ON COMMIT) command on the index.

You can change the problematic index on the logical standby database to not be in ASYNC mode. The index can be set to synchronous or it can be set to manually update.

For more information on XMLIndex, refer to the "Indexing XMLType Data" chapter in the *Oracle XML DB Developer's Guide*.

13 Oracle Data Mining

The Data Mining option is installed with the Enterprise Edition.

Data Mining users must have the CREATE MINING MODEL privilege to create mining models in their own schema. Additional privileges are required for other data mining activities, as described in *Oracle Data Mining Administrator's Guide*.

New data dictionary views for Oracle Data Mining are introduced in Oracle Database 11*g* Release 1 (11.1):

- USER/ALL/DBA_MINING_MODELS

- `USER/ALL/DBA_MINING_MODEL_ATTRIBUTES`

- `USER/ALL/DBA_MINING_MODEL_SETTINGS`

Demo programs that illustrate the Data Mining APIs (PL/SQL and Java) are installed with Oracle Database Companion. Instructions are in the *Oracle Data Mining Administrator's Guide*.

14 Oracle Database Vault

Note the following when working with Oracle Database Vault.

14.1 Configuring Oracle Database Vault

After you install Oracle Database Vault, you need to configure it using Database Configuration Assistant (DBCA). This procedure creates and registers the accounts you need to run Oracle Database Vault.

To configure Oracle Database Vault, execute the following steps:

1. Start Database Configuration Assistant.

2. In the Operations window, select `Configure Database Options`. Click `Next`.

3. In the Database window, select the database where you installed Oracle Database Vault. Click `Next`.

4. In the Database Components window, select both `Oracle Label Security` and `Oracle Database Vault`.

5. In the Oracle Database Vault Credentials window, enter the following information:

   - `Database Vault Owner:` *owner_name*

   - `Database Vault Owner Password:` *password*

   - `Confirm Password:` *password*

   Optionally, select the `Create a Separate Account Manager` check box, and then:

   - `Database Vault Account Manager:` *account_manager_name*

   - `Database Vault Account Manager Password:` *password*

   - `Confirm Password:` *password*

   Click `Next`.

6. Complete the DBCA prompts to configure other Oracle Database components.

15 Oracle Internet Directory

The Oracle Internet Directory product ships only with Oracle Application Server, not the Oracle Database 11*g* Release 1 (11.1) product set. The following information is included because Oracle Network functionality may use Oracle Internet Directory. Many of the administrative activities for Oracle Internet Directory have been consolidated into a single tool, Oracle Internet Directory

Configuration Assistant (OIDCA). OIDCA should be used with Enterprise User Security and Network Names features under these conditions:

1. Enterprise User Security

   - Enterprise User Security only works with Identity Management Realms in this release. You must convert Oracle Contexts used in prior releases to Identity Management Realms using the OIDCA tool.

   - Use OIDCA when creating or updating the ldap.ora configuration file for discovering the Oracle Internet Directory server in the environment. When created with OIDCA, ldap.ora is located in the $ORACLE_HOME/ldap/admin directory on UNIX operating systems and in the ORACLE_HOME\ldap\admin directory on Windows operating systems.

2. Network Names

   - Use OIDCA when creating, upgrading and deleting Oracle Contexts.

   - Use OIDCA when converting an Oracle Context from an earlier release to an Identity Management Realm.

   - Use OIDCA when setting up the ldap.ora configuration file for discovering the Oracle Internet Directory server in the environment.

Note the following items when working with Oracle Internet Directory.

15.1 Using the Oracle Internet Directory Configuration Assistant

The Oracle Internet Directory Configuration Assistant (OIDCA) enables you to create, upgrade, and delete an Oracle Context, configure the file ldap.ora, and convert an Oracle Context to an Identity Management Realm.

The OIDCA syntax is:

```
oidca oidhost=host
      nonsslport=port |
      sslport=SSL Port
      dn=binddn
      pwd=bindpwd
      propfile=properties file
```

To see the usage of OIDCA, enter oidca -help at the command prompt.

15.2 Creating an Oracle Context

The following syntax is used to create an Oracle Context in OIDCA; the parameters are described in the subsequent table.

```
oidca oidhost=host
      nonsslport=port
      sslport=SSL Port
      dn=binddn
      pwd=bindpwd
      mode=CREATECTX
      contextdn=OracleContext DN
```

Parameters	Description
oidhost	OID server host; if not specified, default is localhost

Parameters	Description
nonsslport	OID server port; if not specified, default is 389
sslport	OID SSL port; if not specified, default is 636
dn	OID user, such as cn=orcladmin
pwd	OID user password
mode	Mode of the OIDCA; set to CREATECTX
contextdn	DN under which OracleContext must be created, such as dc=acme,dc=com

Note the following points:

- The contextdn must exist for this operation to be successful.

- This valid DN should not exist in OID: "cn=oraclecontext,dc=acme, dc=com".

- This valid DN must exist in OID: "dc=acme,dc=com".

- The parameters mode and contextdn can also be passed as a properties file.

- Specify the parameter nonsslport=port if you want to perform the operation using non-SSL mode.

- Specify the parameter sslport=sslport if you want to perform the operation using SSL mode.

- Either the nonsslport or the sslport parameter must be specified, but not both.

Functionality

1. The OIDCA verifies that contextdn has a valid DN syntax and that the entry exists in Oracle Internet Directory. Note that the OIDCA cannot create a root OracleContext explicitly. If there is no root Oracle Context, then OIDCA exits with an error.

2. If DN exists, then OIDCA verifies that the Oracle Context already exists.

   - If the Oracle Context already exists and is up-to-date, then OIDCA exits with the message Oracle Context already exists and is up to date.

   - If the Oracle Context already exists, but it is an older version, then OIDCA exits with the message Oracle Context already exists and is of an older version.

   - If the Oracle Context does not exist, then OIDCA creates the Oracle Context under this DN.

15.3 Upgrading an Oracle Context

To upgrade an OracleContext instance, use the following syntax; the parameters are listed in the subsequent table.

```
oidca oidhost=host
     nonsslport=port
     sslport=SSL Port
     dn=binddn
```

```
pwd=bindpwd
mode=UPGRADECTX
contextdn=OracleContext DN
```

Parameters	Description
oidhost	OID server host; if not specified, default is `localhost`
nonsslport	OID server port; if not specified, default is `389`
sslport	OID SSL port; if not specified, default is `636`
dn	OID user, such as `cn=orcladmin`
pwd	OID user password
mode	Mode of the OIDCA; always set to `UPGRADECTX`
contextdn	DN under which `OracleContext` must be created, such as `dc=acme,dc=com`

Note the following points:

- The `contextdn` must contain an `OracleContext` for this operation to be successful.

- The DNs `"cn=oraclecontext,dc=acme,dc=com"` and `"dc=acme,dc=com"` are both valid.

- The parameters `mode` and `contextdn` can also be passed as a properties file.

- Specify the parameter `nonsslport=port` if you want to perform the operation using a non-SSL mode.

- Specify the parameter `sslport=sslport` if you want to perform the operation using SSL mode.

- Either the `nonsslport` or the `sslport` parameter must be specified, but not both.

Functionality

1. OIDCA verifies that the `contextdn` has valid DN syntax and that `OracleContext` exists in Oracle Internet Directory. OIDCA cannot upgrade a root `OracleContext` explicitly. If there is no root `OracleContext`, then OIDCA sends an error message.

2. If `OracleContext` exists under `contextdn`,

   - The OIDCA checks if the `OracleContext` belongs to a realm, in which case it exits with the appropriate message. Note that `OracleContext` instances that belong to a realm cannot be upgraded.

   - The OIDCA verifies that the `OracleContext` is up-to-date, then exits with the message `Oracle Context already exists and is up to date`.

   - If the `OracleContext` is not up-to-date, then the OIDCA upgrades the `OracleContext` under this DN.

15.4 Deleting an Oracle Context

To delete an OracleContext, use the following syntax; the parameters are listed in the subsequent table.

```
oidca oidhost=host
      nonsslport=port
      sslport=SSL Port
      dn=binddn
      pwd=bindpwd
      mode=DELETECTX
      contextdn=OracleContext DN
```

Parameters	Description
oidhost	OID server host; if not specified, default is localhost
nonsslport	OID server port; if not specified, default is 389
sslport	OID SSL port; if not specified, default is 636
dn	OID user, such as cn=orcladmin
pwd	OID user password
mode	Mode of the OIDCA; always set to DELETECTX
contextdn	DN under which OracleContext must be created, such as dc=acme, dc=com

Note the following points:

- The contextdn must contain an OracleContext for this operation to be successful.

- The DNs "cn=oraclecontext, dc=acme, dc=com" and "dc=acme, dc=com" are both valid.

- The parameters mode and contextdn can also be passed as a properties file.

- Specify the parameter nonsslport=port if you want to perform the operation using a non-SSL mode.

- Specify the parameter sslport=sslport if you want to perform the operation using SSL mode.

- Either the nonsslport or the sslport parameter must be specified, but not both.

Functionality

1. OIDCA verifies that the contextdn has valid DN syntax and that OracleContext exists in Oracle Internet Directory.

2. If OracleContext exists under contextdn,

   - The OIDCA checks if the OracleContext belongs to a realm, in which case it exits with the appropriate message. Note that OracleContext instances that belong to a realm cannot be deleted.

   - If OracleContext does not belong to a realm, OIDCA deletes it.

15.5 Configuring the file ldap.ora

To configure the file `ldap.ora`, use the following syntax; the parameters are listed in the subsequent table.

```
oidca oidhost=host
      nonsslport=port
      sslport=SSL Port
      adminctx=Administrative context
      mode=LDAPORA
      dirtype=OID or AD
      -update
```

Parameters	Description
oidhost	OID server host; if not specified, default is `localhost`.
nonsslport	OID server port; determined using discovery APIs.
sslport	OID SSL port; determined using discovery APIs.
mode	Mode of the OIDCA; always set to `LDAPORA`.
dirtype	Directory type; possible values are `OID` and `AD`; mandatory attribute.
adminctx	Default administrative context, such as `dc=acme,dc=com`. If not specified, determined using discovery.
-update	If this flag is specified, then overwrite existing `ldap.ora`; if not, then create `ldap.ora` only if it does not already exist.

Note the following points:

- At least either non-SSL or SSL port must be specified. The other port is discovered.

- The parameters `mode`, `dirtype`, and `adminctx` can also be passed in within a properties file.

Functionality

1. Using the Discovery API, the OIDCA determines all the parameters not specified on the command line.

2. The OIDCA checks for the `ldap.ora` location using Discovery APIs.

   - If `ldap.ora` exists and the `-update` parameter is not specified, then exit with message `ldap.ora exists`.

   - If `ldap.ora` exists and the `-update` parameter is not specified, then update the existing `ldap.ora` using Discovery API.

   - If `ldap.ora` does not exist, create a new `ldap.ora` file in a location in the following order:

     ```
     LDAP_ADMIN
     $ORACLE_HOME/ldap/admin
     ```

15.6 Converting an Oracle Context to an Identity Management Realm

Oracle Database 10*g* entries must be stored in Oracle Internet Directory release 9.0.4 server. An Identity Management Realm release 9.0.4 is also required for Enterprise User Security, a feature of the Oracle Database 10*g*.

To convert an existing `OracleContext` to an Identity Management Realm, use the following syntax. The parameters are listed in the subsequent table. Note that the root of the `OracleContext` object is not converted.

```
oidca oidhost=host
      nonsslport=port
      sslport=SSL Port
      dn=binddn
      pwd=bindpwd
      mode=CTXTOIMR
      contextdn=OracleContext DN
```

Parameters	Description
`oidhost`	OID server host; default is `localhost`
`nonsslport`	OID server port; default is `389`
`sslport`	OID SSL port; default is `636`
`dn`	OID user, such as `cn=orcladmin`
`pwd`	OID user password
`mode`	Mode of the OIDCA; always set to `CTXTOIMR`
`contextdn`	DN under which `OracleContext` must be created, such as `dc=acme,dc=com`

Note the following points:

- The `OracleContext` must exist under the specified `contextdn`.

- The DNs "`cn=oraclecontext,dc=acme,dc=com`" and "`dc=acme,dc=com`" are both valid.

- The parameters `mode` and `contextdn` can also be passed in a properties file.

- Specify the parameter `nonsslport=port` if you want to perform the operation using a non-SSL mode.

- Specify the parameter `sslport=sslport` if you want to perform the operation using SSL mode.

- Either the `nonsslport` or the `sslport` parameter must be specified, but not both.

Functionality

1. The OIDCA checks if `contextdn` has valid DN syntax, and if it contains a valid `OracleContext`.

2. If `OracleContext` exists under `contextdn`,

    - The OIDCA checks if the `OracleContext` belongs to a realm. If it does, then it exits with an appropriate error message.

    - If `OracleContext` does not belong to a realm, OIDCA upgrades it to the latest version, and converts it to a realm.

Note also:

- If the nickname attribute is not cn, configure it as a user configuration attribute using the Oracle Internet Directory Self-Service Console.

- If you want to use the Oracle Internet Directory Self-Service Console to manage the users and groups in the converted realm, you must set up the administrative privileges appropriately. For details, see the *Oracle Internet Directory Administrator's Guide*.

16 Oracle Multimedia

The name Oracle *inter*Media has been changed to Oracle Multimedia in Oracle Database 11*g* Release 1 (11.1). The feature remains the same, only the name has changed. References to Oracle *inter*Media will be replaced with Oracle Multimedia, however some references to Oracle *inter*Media or *inter*Media may still appear in graphical user interfaces, code examples, and related documents in the Oracle Database documentation library for 11*g* Release 1 (11.1).

For additional information, see the Oracle Multimedia readme file located at:

```
$ORACLE_HOME/ord/im/admin/README.txt
```

16.1 Oracle Multimedia Sample Applications

In previous releases, Oracle Multimedia sample applications were available with the Oracle Database distribution media on the Companion CD. In this release, Oracle Multimedia sample applications are available with other examples on the Oracle Database Examples media, which is available for download from OTN. The Oracle Database Examples media is a simple rename of the Companion CD except that it now contains only examples.

Oracle Multimedia User's Guide incorrectly states that the sample applications are available after you install Oracle Multimedia. In addition, Oracle Multimedia demonstration README.txt files incorrectly state that the samples are available from the Companion CD.

17 Oracle OLAP

Consider the following when working with Oracle OLAP:

- The OLAP Option, as an embedded feature of the database, is automatically installed with the Oracle Enterprise Edition Database. When installing the database with the intention of using the OLAP Option, it is recommended that the Data Warehouse configuration type be chosen. This results in the most appropriate default initialization parameters for the database instance.

- Analytic Workspace Manager 11*g* must be used when running Oracle Database 11*g* Release 1 (11.1) in either 10.2 or 11.1 compatibility modes. A 10.2 format analytic workspace may be created by either running on Oracle 10.2 compatibility mode or by choosing the 10.2 cube type when creating a new analytic workspace.

- Oracle Business Intelligence Beans 10*g* and Oracle Discoverer for OLAP 10*g* cannot be used with Oracle OLAP 11.1.0.6.0.

- Upgrading analytic workspaces created in Oracle 10.x to Oracle 11.1 is not supported in this release. (Analytic workspaces created in Oracle 10.x can be used when Oracle 11.1 is in Oracle 10.2 compatibility mode.) For more information, refer to MetaLink Tech Note 445311.1.

- The OLAPSYS schema and the CWM metadata contained within the schema are deprecated in Oracle Database 11*g* Release 1 (11.1). The OLAP API can still query relational tables (ROLAP mode) using data dictionary metadata. For more information, refer to MetaLink Tech Note 445311.1.

- OLAP 10*g* clients connecting to 10*g* style Analytic Workspaces in an 11*g* database should upgrade their Java to version 1.5, as well as upgrade their OLAP API version to 11*g*.

18 Oracle Real Application Clusters

Note the following items when working with Oracle Real Application Clusters (RAC).

Additional Oracle RAC-specific information may also be found in a special readme file located at:

```
$ORACLE_HOME/srvm/doc/README.doc
```

18.1 Changing Host Names

Avoid changing host names after you complete the Oracle Clusterware installation. This is a complex process and it includes adding or deleting domain qualifications. Nodes with changed host names must be deleted from the cluster and added back with the new name.

18.2 Requirements for Rolling Upgrade of Oracle Clusterware

When upgrading Oracle Real Application Clusters from release 10.2.0.1 or 10.2.0.2 to release 11.1, rolling upgrade of Oracle Clusterware will require some additional steps (reference Bug 5198903). Execute the following to successfully complete the rolling upgrade:

1. Upgrade Oracle Clusterware (that is, the CRS home) to release 10.2.0.3, or 10.2.0.2 with CRS Bundle Patch #2 (reference Bug 5256865).

2. Upgrade Oracle Clusterware from release 10.2.0.3 to release 11.1.

Note that each of the Oracle Clusterware upgrades in Steps 1 and 2 are rolling upgrades. Therefore, cluster outage is not required for these upgrades.

There is a similar requirement for rolling upgrade of 10.1.0.2 to 11.1 (reference Bug 5860479). To successfully perform a rolling upgrade of Oracle Clusterware from 10.1.0.2, execute the following:

1. Upgrade Oracle Clusterware (that is, the CRS home) to release 10.1.0.3.

2. Upgrade Oracle Clusterware from release 10.1.0.3 to release 11.1.

The Oracle Clusterware upgrades in Steps 1 and 2 are rolling upgrades, therefore no cluster outage is required.

This is a problem for Oracle Real Application Clusters only. For single-instance database installations with ASM, Oracle Clusterware may be upgraded directly from release 10.1.*x* or 10.2.*x* to release 11.1.

19 Oracle Sample Schemas

Loading of Sample Schemas in locales where the decimal separator is not a period (.) character may result in an error. This only affects the SH schema data. The database creation is successful.

The workaround is to remove the second `CONNECT sh/&pass` statement in the `sh_main.sql` script under `$ORACLE_HOME/demo/schema/sales_history` and run the script manually.

20 Oracle ODBC Driver

The Oracle ODBC Driver Readme file is located at:

`$ORACLE_HOME/odbc/html/ODBCRelnotesUS.htm`

21 Oracle Spatial

The Oracle Spatial readme file supplements the information in the following manuals: *Oracle Spatial Developer's Guide*, *Oracle Spatial Topology and Network Data Models Developer's Guide*, and *Oracle Spatial GeoRaster Developer's Guide*. The Oracle Spatial readme file is located at:

`$ORACLE_HOME/md/doc/README.txt`

22 Oracle Text

Note the following items when working with Oracle Text. You should also check entries for *Oracle Text Application Developer's Guide* in the Documentation Addendum.

22.1 Query Compatible Syntax Values

Chapter 6, titled "CTX_CLS Package", in the *Oracle Text Reference* states under the section titled "Query Compatible Syntax" that the doc_id column is a `NUMBER`. This is correct; however, the values stored in this column must be in the range `0-4294967295`. The values must be stored in an unsigned 32-bit value. This also pertains to `catid`, `catdocid`, and `rescatid`.

22.2 Oracle Text Supplied Knowledge Bases

An Oracle Text knowledge base is a hierarchical tree of concepts used for theme indexing, `ABOUT` queries, and deriving themes for document services. The following Oracle Text services require that a knowledge base be installed:

- Index creation using a `BASIC_LEXER` preference where `INDEX_THEMES=YES`
- `SYNC`ing of an index where `INDEX_THEMES=YES`
- `CTX_DOC.THEMES`
- `CTX_DOC.POLICY_THEMES`
- `CTX_DOC.GIST`
- `CTX_DOC.POLICY_GIST`

- `CTX_QUERY.HFEEDBACK`

- `CTX_QUERY.EXPLAIN`, if using `ABOUT` or `THEMES` with `TRANSFORM`

- `CTX_DOC.SNIPPET` (if using the `ABOUT` operator)

- `CTX_DOC.POLICY_SNIPPET` (if using the `ABOUT` operator)

- `CONTAINS` queries that use `ABOUT` or `THEMES` with `TRANSFORM`

- The Knowledge Base Extension Compiler, `ctxkbtc`

- Clustering and classification services, if themes are specified

If you plan to use any of these Oracle Text features, you should install the supplied knowledge bases, English and French, from the Oracle Database Examples media, available for download on OTN.

Note that you can extend the supplied knowledge bases, or create your own knowledge bases, possibly in languages other than English and French. For more information about creating and extending knowledge bases, see the *Oracle Text Reference*.

For information on how to install products from the Oracle Database Examples media, see the *Oracle Database Examples Installation Guide* specific to your platform.

Supplied Knowledge Bases and Upgrades

Because the supplied knowledge bases are contained on the Oracle Database Examples media, they are not immediately available after an upgrade to Oracle Database 11*g* Release 1 (11.1) Oracle Text features that depend on the supplied knowledge bases available before the upgrade will not function after the upgrade, so you have to install the supplied knowledge bases from the Oracle Database Examples media.

After an upgrade, you must regenerate all user extensions to the supplied knowledge bases. These changes affect all databases installed in the given `$ORACLE_HOME`.

For more information on upgrading Oracle Text and supplied knowledge bases, see the *Oracle Database Upgrade Guide*, Chapter 4, "After Upgrading a Database", section "Upgrading Oracle Text". The *Oracle Text Application Developer's Guide* contains both general instructions for upgrading from previous releases of Oracle Text and information on supplied knowledge bases.

22.3 Oracle Text Indexes Created With Storage Preference Using SecureFiles

Queries on Oracle Text indexes created with storage preference using SecureFiles with `ENCRYPT`, `COMPRESS` or `DEDUPLICATE` enabled may encounter an internal error (reference Bug 6085280).

23 Oracle Ultra Search

Oracle Ultra Search has been deprecated. No new features are implemented in Ultra Search, and Ultra Search will no longer be included as part of future Oracle product sets. In March of 2006, Oracle launched Oracle Secure Enterprise Search (SES). Oracle SES is a faster and more secure product built on the technologies

originally developed for Ultra Search. Customers using Ultra Search are strongly recommended to migrate to Oracle SES.

> **See Also:**   The Oracle Secure Enterprise Search page on the Oracle Technology Network at:
>
> http://www.oracle.com/technology/products/oses/index .html

24 Oracle Warehouse Builder

For late breaking information about Oracle Warehouse Builder, see the *Oracle Warehouse Builder Release Notes.*

25 Oracle Workflow

Oracle Workflow is not shipping with Oracle Database 11*g* Release 1 (11.1).

26 Oracle XML Developer's Kit

Current limitations:

- XML Schema-aware Binary XML - All data values are encoded in their lexical form which is a UTF-8 character sequence.

In 11*g*, Java XDK is supported on JDK 5.0 and above. In addition, the SOAP packages under oracle.soap have been deprecated. The Oracle XML Developer's Kit readme file is located at:

$ORACLE_HOME/xdk/readme.html

27 Oracle XML DB

Note the following when working with Oracle XML DB.

27.1 Database Native Web Services

Database native web services used in an Oracle RAC configuration are not supported.

27.2 NFS Restriction

The Network File System (NFS) protocol support in Oracle XML DB is not supported in Oracle Database 11*g* Release 1 (11.1).

27.3 XML DB Repository Events

For creating a resource based on XDBResconfig.xsd schema (Resource Configuration Schema) in the XML DB Repository, XML schema validation should be turned off by setting event 31150 to level 0x4000.

Event handling code should not contain operations that might render the repository unusable. In addition, the following scenarios should be avoided:

- Creating resources in an event handler that is fired during the creation of another resource.

- Deleting a resource while it is under creation.

Use resource properties, not resource contents, in precondition checks for creation and update events. Preconditions that examine the contents of a resource (for example, /Resource/Contents/) are not evaluated for creation and update events, so events are never fired for resources with such preconditions (reference Bug 5260332).

28 PL/SQL

Note the following when working with PL/SQL.

28.1 DBMS_SCHEDULER PL/SQL Package

Consider the following when working with the DBMS_SCHEDULER PL/SQL package.

28.1.1 Event-Based Jobs

The Oracle Scheduler has support for event-based jobs. These are jobs that are started when a message is enqueued into a database queue. When the database queue used for this purpose is a secure queue, the QUEUE_SPEC attribute of event-based jobs and schedules is a pair of the form *queue_name, agent_name*. The reason an agent has to be specified is to help the scheduler determine which messages the user is allowed to see. In the case of nonsecure queues, if the user has dequeue privileges on a queue then he can dequeue as any agent that is subscribed to the queue. This means that he can see all the messages in the queue. In the case of secure queues, the user has to be granted privileges to not only the queue but to agents as well.

In addition to granting dequeue privileges, the queue owner has to make a call to dbms_aqadm.enable_db_access() to allow the user to dequeue as a specific agent. The agent could be subscribed to the queue using a rule which filters out messages that the user should not see.

The scheduler always subscribes to every queue (secure or otherwise) using its own agent SCHEDULER$_EVENT_AGENT. Since the scheduler runs as user SYS, it can see all the messages in the queue. In the case of secure queues, however, this should not be done since the purpose of secure queues is to allow the queue owner to provide some kind of limited access to the queue to users. Therefore, the scheduler requires an agent name in the QUEUE_SPEC attribute. This agent name is used solely for the purpose of determining which messages the user is allowed to see. The scheduler does not dequeue messages as this agent. When the scheduler receives notification that a message has arrived in a secure queue then it performs the following checks for each event-based job that depends on the queue.

1. It checks to see if the job owner has dequeue privileges on the queue.

2. It checks to see if the agent name provided in the queue spec can be used by the job owner.

3. It checks to see if the agent is currently subscribed to the queue.

4. It checks if the incoming message is visible to the agent.

If all the above checks pass, the scheduler launches the event-based job. Regardless of whether the checks pass or not, the message is dequeued using the agent SCHEDULER$_EVENT_AGENT.

When providing an agent for the QUEUE_SPEC attribute, the user can provide an existing agent name or have a new one created for this purpose. In either case, it is the user's or queue owner's responsibility to ensure that the agent dequeues its messages.

28.1.2 Remote Jobs

The Oracle Scheduler has support for running jobs on remote hosts and transferring files to or from remote hosts. In order to do this, it is first necessary to go through the setup described in the "Enabling and Disabling Remote External Jobs" section of Chapter 28 of the *Oracle Database Administrator's Guide*. This feature also requires that the Oracle XML DB HTTP Server be enabled on the database.

To check whether the Oracle XML DB HTTP Server is enabled, you can use the following command:

```
SQL> SELECT DBMS_XDB.GETHTTPPORT() FROM DUAL;
```

If this statement returns 0, you need to enable the Oracle XML DB HTTP Server on a non-zero port by logging in as SYS and issuing the following commands:

```
SQL> EXEC DBMS_XDB.SETHTTPPORT (port);
SQL> COMMIT;
```

Substitute *port* with the Oracle XML DB HTTP Server port you wish to use.

28.2 UTL_TCP, UTL_HTTP, UTL_SMTP, UTL_MAIL, and UTL_INADDR PL/SQL Packages

A new security measure is introduced in this release for the following network-related PL/SQL packages: UTL_TCP, UTL_HTTP, UTL_SMTP, UTL_MAIL, and UTL_INADDR. The invoker of those packages needs additional privileges to connect to an external host or to resolve the name or the IP address of a host. The packages check the invoker for the necessary privileges only when the calls are made at runtime and raises an exception if the invoker lacks the privileges. This new security measure is implemented by XML DB's access control list (ACL) mechanism and, therefore, requires XML DB to be installed in order to use those packages.

Each external host that a database user wants to connect to or to resolve the name or IP address for from the database is restricted by an access control list (ACL). To grant a user the privileges for the host, the database administrator should create an ACL, add the privileges to the ACL for the user, assign the ACL to the host and commit the changes using the DBMS_NETWORK_ACL_ADMIN PL/SQL package. For example, to give the users SCOTT and ADAMS the permission to connect to www.oracle.com via HTTP (namely to connect to TCP/IP port 80), the database administrator should execute the following:

```
SQL> REM Creates a new ACL and adds SCOTT the privilege to make
TCP connections
SQL> EXECUTE DBMS_NETWORK_ACL_ADMIN.CREATE_ACL('acl_for_oracle.xml', -
> 'ACL for www.oracle.com', 'SCOTT', TRUE, 'connect')
```

```
SQL> REM Adds ADAMS the privilege to the ACL to make TCP connections also
SQL> EXECUTE DBMS_NETWORK_ACL_ADMIN.ADD_PRIVILEGE('acl_for_oracle.xml', -
> 'ADAMS', TRUE, 'connect')

SQL> REM Assigns the new ACL to www.oracle.com for TCP/IP port 80 (HTTP)
SQL> EXECUTE DBMS_NETWORK_ACL_ADMIN.ASSIGN_ACL('acl_for_oracle.xml', -
> 'www.oracle.com', 80)

SQL> REM Commits to make the ACL take effect
SQL> COMMIT
```

The invoker of the UTL_TCP, UTL_HTTP, UTL_SMTP, and UTL_MAIL packages needs the 'connect' privilege to make TCP/IP, HTTP, or SMTP connections to the external host. The invoker of the UTL_INADDR package needs the 'resolve' privilege to resolve the name or the IP address of the external host. Note that those privileges are not granted through the GRANT SQL statement but through the DBMS_NETWORK_ACL_ADMIN package.

The current ACL assignment to external hosts and the privileges currently defined in the ACLs are shown through the system catalog views DBA_NETWORK_ACLS and DBA_NETWORK_ACL_PRIVILEGES.

The invokers of other database components that use those PL/SQL packages to perform network operations from the database, which are XML DB's HttpUriType, Oracle Multimedia (formerly *inter*Media), and Spatial, are subject to the same network permission check and need the same privileges.

28.3 DBMS_SQL Package

In Oracle Database 11*g* Release 1 (11.1), Oracle introduces a number of enhancements to DBMS_SQL to improve the security of the package:

- Prevent guessing of open cursor numbers

  A new error, ORA-29471, will be raised when any DBMS_SQL subprogram is called with a cursor number that does not denote an open cursor. When the error is raised, an alert is issued to the alert log and DBMS_SQL becomes inoperable for the life of the session.

  If the actual value for the cursor number in a call to IS_OPEN does denote a cursor that is currently open in the session, the return value is TRUE. If the actual is null, the return value is FALSE. Otherwise, you get the ORA-29471. error.

  Note that the DBMS_SQL.OPEN_CURSOR function is the only DBMS_SQL subprogram that has no formal parameter for the cursor number. Rather, it returns a cursor number. Therefore, it is not within the scope of the rules.

- Prevent inappropriate use of a cursor

  Cursors are now better protected from security breaches that subvert known, existing cursors.

  Checks are always made when binding and executing. Optionally, checks may be performed for every single DBMS_SQL subprogram call. The check is:

  - current_user is the same on calling the subprogram in question as it was on calling the most recent parse.

  - The enabled roles on calling the subprogram must be a superset of the enabled roles on calling the most recent parse.

As is always the case, for definer's right subprograms, roles are irrelevant.

If either check fails, `ORA-29470` is raised.

The mechanism for defining when checks are performed is a new overload for the `OPEN_CURSOR` subprogram which takes a formal parameter, `security_level`, with allowed values `NULL`, `1` and `2`.

When `security_level = 1` (or is `NULL`), the checks are made only when binding and executing. When `security_level = 2`, the checks are always made.

This security regime is stricter than in 10.2 and previous releases. As a consequence, users of `DBMS_SQL` may encounter runtime errors on upgrade. While the regime makes for more secure applications, users may want to relax the security checks temporarily as they migrate to 11.1. If so, please consult with Oracle Support Services on steps to relax the security checks.

28.4 UTL_FILE Package

The `UTL_FILE` package no longer opens a file if that file is a symbolic link. This new restriction closes a known security hole in the `UTL_FILE` package.

If this security restriction poses an undue burden during migration, contact Oracle Support Services for assistance.

28.5 Interoperability Between Releases

Interoperability between an 11.1 database or Forms client and a 10.1 or 10.2 database requires a minimum patchset level of 10.1.0.5 (for 10.1) or 10.2.0.2 (for 10.2).

An attempt to reference a 10.1 or 10.2 PL/SQL unit or view under the following circumstances fails with a PLS-801[55916] error unless the 10.1 or 10.2 environment has been patched to the correct level:

- A PL/SQL unit, anonymous block, trigger, call statement, or SQL statement on an 11.1 database invokes a PL/SQL unit on a 10.1 or 10.2 database across a database link.

- A PL/SQL unit, anonymous block, trigger, or call statement on an 11.1 database references a view on a 10.1 or 10.2 database across a database link and the view directly or indirectly references a PL/SQL function or an object type.

- An 11.1 Forms client invokes a PL/SQL unit in a 10.1 or 10.2 database using RPC.

To avoid the PLS-801[55916] error, a minimum patchset level of 10.1.0.5 (for 10.1) or 10.2.0.2 (for 10.2) is required.

There is no interoperability problem between 10.1 and 10.2 environments.

29 Pro*C

The Pro*C readme file is located at:

```
$ORACLE_HOME/precomp/doc/proc/readme.doc
```

30 Pro*COBOL

The Pro*COBOL readme file is located at:

```
$ORACLE_HOME/precomp/doc/procob2/readme.doc
```

31 SQLJ

SQLJ in Oracle Database 11*g* Release 1 (11.1) is supported with JDK 5 and JDK 6.

32 SQL*Plus

The SQL*Plus readme file is located at:

```
$ORACLE_HOME/sqlplus/doc/README.htm
```

33 Summary Management

Note the following items when working with Summary Management.

33.1 Query Rewrite

The following items apply to Query Rewrite.

33.1.1 Fine Grained Auditing (FGA)

If Fine Grained Auditing (FGA) is enabled on a table in the query, Query Rewrite will not occur for this query.

33.1.2 Use of PARTITION Clause

Query rewrite does not occur for queries that use the PARTITION clause in the FROM clause to access table partitions. In order for query rewrite to rewrite such queries, the PARTITION clauses must first be converted into equivalent selection predicates and added to the WHERE clause.

33.2 Feature Availability

The creation and refresh features of materialized views are supported in both the Standard and Enterprise Editions. However, query rewrite and materialized view advice from the SQL Access Advisor are available in the Enterprise Edition only.

33.3 NLS Parameters

When using or refreshing certain materialized views, you must ensure that your NLS parameters are the same as when you created the materialized view. Materialized views that fall under this restriction contain the following constructs:

1. **Expressions that may return different values, depending on NLS parameter settings**

   It is recommended to write such expressions in the NLS-independent way. For example:

   ```
   (date > DATE '2003-01-02')
   ```

Or:

```
(rate <= 2.150)
```

2. **Equijoins where one side of the join is character data**

   The result of this equijoin depends on collation and this can change on a session basis, giving an incorrect result in the case of query rewrite or an inconsistent materialized view after a refresh operation.

3. **Expressions that generate internal conversion to character data in the select list of a materialized view, or inside an aggregate of a materialized aggregate view**

   This restriction does not apply to expressions that involve only numeric data; for example, `a+b` where `a` and `b` are numeric values.

34 Streams

Note the following when working with Streams.

34.1 Propagation from Oracle9*i* Release 9.2 to Oracle Database 11*g* Release 1 (11.1) Returns Error ORA-25334

Propagation from Oracle9*i* Release 9.2 to Oracle Database 11*g* Release 1 (11.1) results in error `ORA-25334` unless the patch to Bug 4285404 has been applied to the Oracle9*i* Release 9.2 database.

34.2 Streams Apply Handler Modifications Necessary for Handling New Error Messages That Replace ORA-1403 Errors

Customized DML and error handlers for Streams require modification to catch the additional Oracle errors ORA-26786 and ORA-26787 in place of the `ORA-01403 No data found` message. An ORA-26787 error is raised if the row to be updated or deleted does not exist in the target table. An ORA-26786 error is raised when the row exists in the target table, but the values of some columns do not match those of the LCR.

34.3 Streams Advanced Queuing

Subscription names for Advanced Queuing notification will become canonical. Thus, registrations for `scott.queue1:sub` and `SCOTT.QUEUE1:SUB` are for the same entity and are represented in canonical form as `"SCOTT"."QUEUE1":"SUB"`.

34.4 DBMS_RULE_ADM Operation Privileges

New in Oracle Database 11*g* Release 1 (11.1), the DBMS_RULE_ADM package might require that the caller be specifically granted the privilege to perform the DBMS_RULE_ADM operation (reference Bug 5523578).

For the short term, if needed, the previous behavior can be restored by setting event 25476 to any nonzero level. However, usage of this event may be deprecated in a future release, therefore it is recommended that you grant the relevant privileges should DBMS_RULE_ADM return a security-related error.

35 Time Zones

Consider the following when working with time zones.

35.1 Daylight Saving Transition (DST)

The Daylight Saving Transition data for all regions has been updated incorporating the rules defined up to and including March 2006. Before upgrading your database to Oracle Database 11*g* Release 1 (11.1), refer to the utltzuv2.sql script located under $ORACLE_HOME/rdbms/admin/ to determine whether or not existing database data will be affected by transitioning to the new version of the Daylight Saving Transition. Comments at the beginning of the script file and in the *Oracle Database Globalization Support Guide* contain further information regarding the issue.

You have to run the utltzuv2.sql script provided with Oracle Database 11*g* Release 1 (11.1); however, the database should still run in version 10.1 or 10.2. Before running the script, copy the file timezdif.csv from $ORACLE_HOME/oracore/zoneinfo directory that is located in the 11*g* Oracle Home to the same directory in the 10*g* Oracle Home.

35.2 utlu111i.sql and Time Zone File V4

There is a known issue with the Pre-Upgrade Information, utlu111i.sql, script when you run it on database release 10.2.0.3.0. Even if you have already run the utltzuv2.sql script as described in Section 35.1, "Daylight Saving Transition (DST)" after you run the utlu111i.sql script, it gives a warning stating that you must upgrade to time zone file version 4.

To workaround this issue, restart the database after running the utlu111i.sql script. The time zone file version changes to 4. Rerun the utlu111i.sql script. The warning does not appear and this issue is resolved.

36 Utilities

Note the following items when working with utilities.

36.1 Original Export/Import Support

The original Export utility is no longer supported for general use. The original Import utility is still supported. However, Data Pump Export and Data Pump Import are the recommended and fully supported utilities for exporting and importing data in Oracle Database 11*g* Release 1 (11.1)

37 Documentation Addendum

This section contains corrections to the following Oracle Documentation for this release:

- Oracle Data Guard Concepts and Administration
- Oracle Database Administrator's Guide
- Oracle Database Concepts
- Oracle Database Heterogeneous Connectivity Administrator's Guide

- Oracle Database New Features Guide, 11g Release 1 (11.1)

- Oracle Database Performance Tuning Guide

- Oracle Database PL/SQL Packages and Types Reference

- Oracle Database Reference

- Oracle Ultra Search Administrator's Guide

- Oracle Ultra Search Online Help

- Oracle Database New Features Guide, 10g Release 2 (10.2)

37.1 Oracle Data Guard Concepts and Administration

The following sections describe late-breaking changes that apply to the *Oracle Data Guard Concepts and Administration* manual.

37.1.1 Performing a Rolling Upgrade

There is a missing action item in Step 6 of Section 12.6 titled "Performing a Rolling Upgrade With an Existing Physical Standby Database." The correct set of actions to take for Step 6 are:

Mount database A:

```
SQL> ALTER DATABASE MOUNT;
```

Archive the current log file at the new primary database (B), and ensure that it is registered at database A. This action ensures that database A is aware of the current incarnation at database B. Once you have verified this, you can start the managed recovery process at database A:

```
ALTER DATABASE RECOVER MANAGED STANDBY DATABASE USING CURRENT LOGFILE
   DISCONNECT FROM SESSION;
```

37.1.2 Flashing Back a Failed Primary Database into a Logical Standby Database

Oracle Data Guard Concepts and Administration contains incorrect information in section 13.2.2. This section provides the correct steps. (In these steps, variables for which you must provide values are in italics.)

These steps assume that the Data Guard configuration has already completed a failover involving a logical standby database and that Flashback Database has been enabled on the old primary database. This procedure brings the old primary database back into the Data Guard configuration as a new logical standby database without having to formally instantiate it from the new primary database.

Step 1 Determine the flashback SCN and the recovery SCN.

The flashback SCN is the SCN to which the failed primary database will be flashed back. The recovery SCN is the SCN to which the failed primary database will be recovered. Issue the following query on the new primary to identify these SCNs:

```
SQL> SELECT merge_change# AS FLASHBACK_SCN, processed_change# AS RECOVERY_SCN
 2> FROM DBA_LOGSTDBY_HISTORY
 3> WHERE stream_sequence# = (SELECT MAX(stream_sequence#)-1
 4> FROM DBA_LOGSTDBY_HISTORY);
```

Step 2 Flash back the failed primary database to the flashback SCN identified in Step 1.

```
SQL> FLASHBACK DATABASE TO SCN flashback_scn;
```

Step 3 Convert the failed primary into a physical standby, and remount the standby database in preparation for recovery.

```
SQL> ALTER DATABASE CONVERT TO PHYSICAL STANDBY;
SQL> SHUTDOWN IMMEDIATE;
SQL> STARTUP MOUNT;
```

Step 4 Identify the logfiles on the new primary that contain redo within range [flashback SCN, recovery SCN].

The logfiles identified by the following query are significant because they are the only "versions" of the archived logfiles that can safely recover the failed primary database. If the logfiles returned from the following query cannot be registered in Step 5, the failed primary database can never be revived as a logical standby database. In such a case, a logical standby database will have to be created from the new primary database.

```
SQL> SELECT file_name FROM DBA_LOGSTDBY_LOG
  2> WHERE first_change# <= recovery_scn
  3> AND next_change#  > flashback_scn;
```

Step 5 Register all logfiles returned from Step 4 with the physical standby (failed primary).

```
SQL> ALTER DATABASE REGISTER LOGFILE 'files_from_step _4';
```

Step 6 Recover until the recovery SCN identified in Step 1.

```
SQL> RECOVER MANAGED STANDBY DATABASE UNTIL CHANGE recovery_scn;
```

Step 7 Enable the database guard.

```
SQL> ALTER DATABASE GUARD ALL;
```

Step 8 Activate the physical standby to become a primary database.

```
SQL> ALTER DATABASE ACTIVATE STANDBY DATABASE;
```

Step 9 Open the database.

```
SQL> ALTER DATABASE OPEN;
```

Step 10 Create a database link to the new primary, and start SQL Apply.

```
SQL> CREATE PUBLIC DATABASE LINK mylink
  2> CONNECT TO system IDENTIFIED BY password
  3> USING 'service_name_of_new_primary_database';

SQL> ALTER DATABASE START LOGICAL STANDBY APPLY NEW PRIMARY mylink;
```

The role reversal is now complete.

37.2 Oracle Database Administrator's Guide

This section contains corrections to the *Oracle Database Administrator's Guide*.

37.2.1 Size of SYSAUX Tablespace

In Chapter 12, "Managing Tablespaces", section "Controlling the Size of the SYSAUX Tablespace" states that a system with an average of 30 concurrent active sessions may require approximately 200 MB to 300 MB of space for its Automatic Workload Repository data. The 200 MB to 300 MB estimate is valid for a system with an average of 10 (rather than 30) concurrent active sessions.

The following table provides guidelines on sizing the SYSAUX tablespace, based on the system configuration and expected load.

Parameter/Recommendation	Small	Medium	Large
Number of CPUs	2	8	32
Number of concurrently active sessions	10	20	100
Number of user objects: tables and indexes	500	5,000	50,000
Estimated SYSAUX size at steady state with default configuration	500 MB	2 GB	5 GB

37.2.2 Running Database Configuration Assistant (DBCA) in Silent Mode

In Chapter 2, "Creating an Oracle Database", the following information should be included:

Silent mode does not have a user interface (other than what you initially input on the command line) or user interaction. It outputs all messages, including information, errors, and warnings, to a log file.

From the command line, enter the following to see all of the DBCA options that are available when using silent mode:

```
dbca -help
```

The following sections contain examples that illustrate the use of silent mode.

DBCA Silent Mode Example 1: Creating a New Database   To create a clone database, enter the following on the command line:

```
% dbca -silent -createDatabase -templateName Transaction_Processing.dbc
-gdbname ora11g -sid ora11g -datafileJarLocation
/private/oracle11g/ora11g/assistants/dbca/templates -datafileDestination
/private/oracle11g/ora11g/oradata -responseFile NO_VALUE
-characterset WE8ISO8859P1
```

DBCA Silent Mode Example 2: Creating a Seed Template   To create a seed template, enter the following on the command line:

```
% dbca -silent -createCloneTemplate -sourceDB ora11g -sysDBAUserName
sys -sysDBAPassword change_on_install -templateName copy_of_ora11g.dbc
-datafileJarLocation /private/oracle/ora11g/assistants/dbca/templates
```

37.3 Oracle Database Concepts

In the section titled *Other Oracle Database Background Processes* in Chapter 9 of the *Oracle Database Concepts*, the list item that discusses ORB should read as follows:

ARB*n* performs the actual rebalance data extent movements in an Automatic Storage Management instance. There can be many of these at a time, called ARB0, ARB1, and so forth.

37.4 Oracle Database Heterogeneous Connectivity Administrator's Guide

The following information should be removed from Chapter 4, "Using Heterogeneous Services Agents", section "Determining the Heterogeneous Services Parameters":

> The Distributed Access Manager has a refresh capability available through the menu and toolbar that allows users to rerun queries if necessary and update the data. When the data is refreshed, the tool verifies that the set of registered agents remains the same. If it is not, the global view is updated. See *Oracle Enterprise Manager Administrator's Guide* and online help for more information about the Distributed Access Manager.

37.5 Oracle Database New Features Guide, 11*g* Release 1 (11.1)

The following corrections should be noted when referring to the *Oracle Database New Features Guide*.

Section 1.2.1.1 Browser-Based Enterprise Manager Integrated Interface for LogMiner   This section should include a statement to the effect that the task-based work flows enable log mining and are integrated with Flashback transactions.

Section 1.5.1.1 Enhanced Oracle RAC Monitoring and Diagnostics in Enterprise Manager   This section should also mention that there are improvements to service-based monitoring and to Summary and Tile-based views for monitoring performance metrics.

Section 1.5.1.2 Enhanced Oracle Real Application Clusters Configuration Assistants   This section should also mention that the `rconfig` utility is enhanced to be able to convert single-instance ASM to clustered ASM. This completes the functionality in release 10*g* where `rconfig` was able to convert a single-instance database to Oracle RAC.

Section 1.7.1.2 Hang Manager   The first paragraph in this section states:

> The Hang Manager automatically detects, analyzes, and dumps diagnostic information for hangs in Oracle Database environments, including Oracle RAC and ASM databases. `V$` views are provided to allow users to see hangs in the system and their current status.

The last sentence in that paragraph is incorrect. There are no `V$` views associated with Hang Manager.

37.6 Oracle Database Performance Tuning Guide

In Chapter 10 (*Instance Tuning Using Performance Views*) of the *Oracle Database Performance Tuning Guide*, the following text should appear:

Oracle Database 11*g* Release 1 (11.1) introduces a change in the way wait counts and time outs are accumulated for wait events (for example, in the `V$SYSTEM_EVENT` view).

Within Oracle, continuous waits for certain types of resources (such as enqueues) are internally broken into a set of shorter wait calls. In releases prior to 11.1, each individual internal wait call was counted as a separate wait. Starting with 11.1, a

single resource wait is recorded as a single wait, irrespective of the number of internal time outs experienced by the session during the wait.

This change allows Oracle to display a more representative wait count, and an accurate total time spent waiting for the resource. Time outs now refer to the resource wait instead of the individual internal wait calls.

As the way waits and time outs are measured has changed, this also affects the average wait time, and the maximum wait time.

For example, there is a problem in the database that a user session must wait for an enqueue it requires (for example, a TX row lock to update a single row in a table) before it can continue processing. Assume it takes 10 seconds to acquire the enqueue. From the sessions perspective, it begins the enqueue wait. Internally to Oracle, this enqueue wait is broken down into 3-second wait calls. In this case, there will be three 3-second wait calls, followed by one 1-second wait call.

In prior releases, the `V$SYSTEM_EVENT` view would represent this wait scenario as follows:

- `TOTAL_WAITS`: 4 waits (three 3-second waits, one 1-second wait)
- `TOTAL_TIMEOUTS`: 3 time outs (the first three waits time out and the enqueue is acquired during the final wait)
- `TIME_WAITED`: 10 seconds (sum of the times from the 4 waits)
- `AVERAGE_WAIT`: 2.5 seconds
- `MAX_WAIT`: 3 seconds

In Oracle Database 11*g* Release 1 (11.1), this wait scenario is represented as:

- `TOTAL_WAITS`: 1 wait (one 10-second wait)
- `TOTAL_TIMEOUTS`: 0 time outs (the enqueue is acquired during the resource wait)
- `TIME_WAITED`: 10 seconds (time for the resource wait)
- `AVERAGE_WAIT`: 10 seconds
- `MAX_WAIT`: 10 seconds

The following common wait events are affected by this change:

- Enqueue waits (for example, `enq: <name> - <reason>` waits)
- Library cache lock waits
- Library cache pin waits
- Row cache lock waits

Statistics affected are listed below:

- Wait counts
- Wait time outs
- Average wait time
- Maximum wait time

Views affected are listed below:

- `V$EVENT_HISTOGRAM`

- V$EVENTMETRIC

- V$SERVICE_EVENT

- V$SEERVICE_WAIT_CLASS

- V$SESSION_EVENT

- V$SESSION_WAIT

- V$SESSION_WAIT_CLASS

- V$SESSION_WAIT_HISTORY

- V$SYSTEM_EVENT

- V$SYSTEM_WAIT_CLASS

- V$WAITCLASSMETRIC

- V$WAITCLASSMETRIC_HISTORY

37.7 Oracle Database PL/SQL Packages and Types Reference

The listno parameter of the DBMS_UTILITY was inadvertently excluded from the *Oracle Database PL/SQL Packages and Types Reference*. For example, the GET_PARAMETER_VALUE function should read as follows:

GET_PARAMETER_VALUE Function

This function gets the value of specified init.ora parameter.

Syntax

```
DBMS_UTILITY.GET_PARAMETER_VALUE (
    parnam       IN           VARCHAR2,
    intval       IN OUT       BINARY_INTEGER,
    strval       IN OUT       VARCHAR2,
    listno       IN           BINARY_INTEGER DEFAULT 1)
  RETURN BINARY_INTEGER;
```

Parameters

Parameter	Description
parnam	Parameter name.
intval	Value of an integer parameter or the value length of a string parameter.
strval	Value of a string parameter.
listno	List item number. If retrieving parameter values for a parameter that can be specified multiple times to accumulate values, use this parameter to get each individual parameter.

37.8 Oracle Database Reference

The text for the SGA_MAX_SIZE initialization parameter in the *Oracle Database Reference* should include the following:

When either MEMORY_TARGET or MEMORY_MAX_TARGET is enabled, SGA_MAX_SIZE default value is set to the larger of the two specified parameters

on non-Windows 32-bit operating system. On Windows 32-bit operating system, due to address space pressure, the default value of SGA_MAX_SIZE is calculated based on the total available virtual address space along with MEMORY_TARGET and MEMORY_MAX_TARGET.

To calculate the value on Windows 32-bit, SGA_MAX_SIZE larger of:

60% of MEMORY_TARGET if set and
60% of MEMORY_MAX_TARGET if set and
25% of total available virtual address space

37.9 Oracle Ultra Search Administrator's Guide

The following note should be included:

If you change the crawler log file directory or the cache directory on a non-Windows system, make sure that the directory permission is set to 700. Only the person who installed the Oracle software should be allowed access to this directory.

37.10 Oracle Ultra Search Online Help

The Attributes page of the Oracle Ultra Search online help states that for Web or file data sources, you can map an HTML metatag to a search attribute in either 'String', 'Date', or 'Number' data types. This is incorrect. This is only supported for 'String' data types.

37.11 Oracle Database New Features Guide, 10g Release 2 (10.2)

The Oracle Database New Features Guide for 10g Release 2 (10.2) incorrectly documented the value MAX for the DB_BLOCK_CHECKSUM initialization parameter. The correct value is FULL (reference Bug 5880145).

38 Open Bugs

This section lists known bugs for this release. A supplemental list of bugs may be found as part of the release documentation specific for your platform.

38.1 Auto-Task Known Bugs

Bug 6129071
Selecting DBA_AUTOTASK_CLIENT view may consume a large amount of CPU resources.

Workaround   None.

38.2 Automatic Storage Management (ASM) Known Bugs

Bug 6275904
ASM only installation fails to launch Database Configuration Assistant.

Workaround   Execute one of the following:

- Configure `/dev/shm` properly
- Set `MEMORY_TARGET=0` in the initialization parameter file to disable Automatic Memory Management.

Bug 6244751

`ASMCMD CP` fails when copying multiple files.

Workaround Specify one source file at a time.

Bug 6197966

When upgrading Automatic Storage Management (ASM) from 10.*x* to Oracle Database 11*g* Release 1 (11.1), if ASM is running at the time the upgrade is attempted, the installer prompts you to shut down ASM and all databases using ASM storage before proceeding with the install and upgrade. If you shut down ASM and all databases using ASM, but leave CSS running, you will receive the following error when you click NEXT:

```
A connection to the Automatic Storage Management (ASM) instance on this
system cannot be established. To ensure proper connection, the operating
system user performing this install (orauser) must be a member of the OSDBA
group of the ASM instance. See the installation guide for more information on
the proper system setup required for running ASM and database instances as
separate operating system users.
```

Workaround When prompted to shut down ASM and all databases using ASM, you should also shut down CSS. Then, cancel out of the installation and start the installer again.

Bug 6162682

DBUA upgrade of Oracle 10*g* database to Oracle 11*g* database fails with the following error:

```
ORA-01017: invalid username/password; logon denied
```

This error occurs if ASM is already upgraded to 11*g* and ASM is running as a different user than the owner of the Oracle binary for the database `ORACLE_HOME` and database software owner is not a member of OSASM.

Workaround Before starting the database upgrade, add the database software owner to the OSASM group. After the upgrade is complete, remove the database software owner from the OSASM group.

Bug 5996064

`ASMCMD CP` fails to copy the file when a relative path is specified.

Workaround Specify the full path to the source and destination.

38.3 Database Configuration Assistant (DBCA) Known Bugs

Bug 5195130

When any database is installed with database configuration type as `Advanced`, during DBCA even though the user selects the Sample Schemas, the final HTML Confirmation dialog screen shows the Sample Schemas selection as `False`. This

does not affect the Sample Schemas functionality because they are installed and configured after the database creation completes.

Workaround None. This observation can be safely ignored.

38.4 Database Resident Connection Pool (DRCP) Known Bugs

Bug 6188988
Server result cache does not work with DRCP.

Workaround Set `RESULT_CACHE_MAX_SIZE=0` in the initialization parameter file.

Bug 6134515
Loopback database links using the bequeath protocol (BEQ) do not work with DRCP.

Workaround Use TCP/IPC protocol for loopback links.

38.5 Java in Oracle Database Known Bugs

Bug 6277149
The Oracle Java VM JMX Management Bean fails to initialize and returns the following error:

```
ORA-29516: Aurora assertion failure: Assertion failure at eoxdebug.c:104
jonom_initialize is not yet implemented
```

Workaround None.

38.6 NET Configuration Assistant (NETCA) Known Bugs

Bug 5954282
After database installation, the NET Configuration Assistant is launched. On the Naming Methods Configuration page, some characters may appear truncated at the end of each line on the default window. This happens in several non-English locales.

Workaround Enlarge the window using the mouse to display more characters.

38.7 Oracle Advanced Security Known Bugs

Bug 6274073
The PKCS11 functionality does not work in Oracle Wallet Manager and `orapki` tool.

Workaround: None.

Bug 6264536

Products using SSL cannot run in FIPS mode as FIPS 140-2 functionality does not work out of the box.

Workaround: None.

38.8 Oracle Application Express Known Bugs

Refer to "Open Bugs and Known Issues" in *Oracle Database Application Express Release Notes*.

38.9 Oracle Call Interface (OCI) Known Bugs

Bug 6317721

For long running OCI applications in which client result cache is enabled, the values in `client_result_cache_stats$` may wrap around.

Workaround   None.

Bug 6221713

If the OCI application process having client result cache application does not make database server roundtrips for an extended time (for example, 10 minutes or more), the application may see the cached results invalidated and reloaded on a subsequent roundtrip, thus decreasing performance. The `client_result_cache_stats$` will show many invalidations after a subsequent roundtrip to the server.

Workaround   Execute one of the following:

- Set Event 29974, Level 333 to avoid this behavior.

- Increase the client result cache lag.

38.10 Oracle Clusterware Known Bugs

Bug 4433140

If you are installing Oracle Clusterware as a user that is a member of multiple operating system groups, the installer installs files on all nodes of the cluster with group ownership set to that of the user's current active or primary group. However, in some cases, group ownership of a small number of files is set incorrectly to the first group that the user is a member of rather than the current active group. In the example output of `/usr/bin/id` below, the current active or primary group is `dba` while the first group that the user is a member of is `ioracle`. This is determined by the order in which groups are listed in the file `/etc/group`.

uid=500(oracle)
gid=8000(dba)
groups=7500(ioracle),8000(dba)

Workaround: Perform any one of the following actions:

- Ensure that the first group listed in the file /etc/ group is the current active group.

- Invoke the Oracle Clusterware installation using the following additional command line option, to force the installer to use the proper group when setting group ownership on all files:

  ```
  runInstaller s_usergroup=current_active_group
  ```

38.11 Oracle Configuration Manager Known Bugs

Bug 5929125

OCM does not support shared Oracle Home in Oracle Database 11*g* Release 1 (11.1). Support is planned for a future release.

Workaround   None.

38.12 Oracle Data Guard Known Bugs

Bug 2795200

Distributed transaction states are not preserved after failover involving a logical standby database. The state of an in-doubt transaction at the primary database is not preserved in the logical standby database on a failover or switchover.

Workaround   None.

38.13 Oracle Data Pump Known Bugs

Bug 6081425

When using Data Pump to import data from an Oracle Database 10.1 or earlier release into a 10.2 or later release, the import fails with error ORA-01403. The specific problem is when a table pre-exists and the table uses a feature that is not in 10.1, such as column-level Transparent Data Encryption columns (as in 10.2) or Tablespace Encryption (as in 11.1).

Workaround: Import into a different schema and INSERT ... SELECT into the table with the 11*g* feature enabled.

Bug 5861640

Data Pump import/export cannot be used for a table on which has XMLIndex has been defined.

Workaround   Drop the XMLIndex before exporting and re-create it after importing.

38.14 Oracle Database Vault Known Bugs

Bug 6311859

Configuring Database Vault might hang if you register the database with OID and configure Oracle Label Security and Database Vault at the same time.

Workaround   Register the database with OID first. Then, restart DBCA to configure Oracle Label Security and Database Vault.

Bug 6258295

DVCA `-action addlanguages` option unlocks the DVSYS account to add languages. The account remains unlocked even after the DVCA task is complete.

Workaround   Manually lock DVSYS account after executing DVCA `-action addlanguages` option.

38.15 Oracle Enterprise Manager Configuration Assistant Known Bugs

Bug 6320584

If an Oracle RAC database is managed by 10.2 Grid Control, and an `add instance` operation is performed to add an instance on the remote node, the Enterprise Manager configuration fails to register the targets of the newly added instance to 10.2 Grid Control.

Workaround   Run the following commands on the node to which the new database instance has been added:

```
setenv ORACLE_HOME oracle_home
setenv ORACLE_SID sid-of-newly-added-instance
run $ORACLE_HOME/bin/emctl config agent addcentralagent central-agent-home
database-oracle-home
```

38.16 Oracle Enterprise Manager Database Control Known Bugs

Bug 6320845

For Database Replay, the Automatic Workload Repository (AWR) Compare Period Report shown in the browser window may not be the report for the selected capture or replay if there is more than one replay for a given capture.

Workaround   After the AWR Compare Period Report is generated, right click on the browser window and select the menu item that gives the address (URL) for the page. Copy and paste this address into the address bar of a new browser window to see the correct report.

Bug 6319054

When applying a patch using the Apply Patch feature with a browser on a non-English locale, the Select Patches page shows a version mismatch error.

Workaround   Set the browser language to English for this page.

Bug 6278749

Database patching procedure from Enterprise Manager Database Control does not support the following patching scenarios:

- Patching of single-instance database with ASM installed in the same Oracle Home.

- Patching of single-instance database with multiple instances running out of the same Oracle Home.

Workaround None.

Bug 6274413

Under certain conditions, an SQL error is returned while creating encrypted tablespaces in Oracle Enterprise Manager if certain Storage options are also selected. This happens due to the incorrect ordering of storage clauses in the SQL statement generated.

Workaround Take the following steps:

1. Click on the `Show SQL` button.

2. Copy the SQL.

3. Remove the repeated keyword, `DEFAULT`, and rearrange the storage clauses.

4. Execute the query using SQL*Plus.

Bug 6266117

During upgrade of 10.2.0.3 database to Oracle Database 11*g* with 2K block size using DBUA, the following error may show up in the Oracle server log:

```
ORA-01404: ALTER COLUMN will make an index too large
```

Workaround This error can be safely ignored as the upgrade will complete successfully. It will eventually run another piece of code which will create the table in the right way and, therefore, no Enterprise Manager functionality will be impacted. There is no feature loss with this error.

Bug 6262682

When converting a single-instance database to a Oracle RAC database using the `rconfig` utility, and if the single-instance database has Database Control configured, Oracle recommends de-configuring Database Control prior to conversion so the converted database will have Oracle RAC Database Control configured.

Workaround The following steps can be taken:

- De-configure Database Control on the single-instance database using the following command:

  ```
  emca -deconfig dbcontrol db
  ```

- Run `rconfig` utility to convert the single-instance database to Cluster Database.

- Run DBCA to configure Database Control for Cluster Database.

Bug 6226229

Some steps failed when configuring a materialized view.

Workaround Save the `Setup Materialized View Site` SQL script from the `Show SQL` page and execute the steps that have failed using appropriate

credentials. You have to log in as materialized view site administrator to configure a materialized view.

Bug 6215796

The create template step failed.

Workaround   Get the `Create Template` SQL script from the `Show SQL` page and execute using appropriate credentials. You must log in as replication administrator to create a template.

Bug 6200122

When you create a partitioned table and select compress option as `ENABLED ON ALL OPERATIONS`, the table will be created correctly with the compression option. However, edit, view, create like and generate DDL will display it as `FOR DIRECT_LOAD OPERATIONS`. This bug only applies to partition table level compression. Compression works properly for other tables, table partition, and tablespace.

Workaround   Click on `Show SQL`, replace `FOR DIRECT_LOAD OPERATIONS` with `ENABLED ON ALL OPERATIONS` and execute through SQL*Plus.

Bug 6196406

Database Configuration Assistant (DBCA) may fail to configure Oracle Enterprise Manager Database Control if executed in Turkish operating system locale. The message `Error uploading configuration data to the repository` is reported.

Workaround   After the database creation, change the operating system session locale to English and configure Oracle Enterprise Manager Database Control manually using the EMCA tool. For example, in Linux `csh` shell, run:

```
$ setenv LC_ALL en_US
$ $ORACLE_HOME/bin/emca -config dbcontrol db -repos recreate [-cluster]
```

See *Oracle Database Utilities* for further information about the EMCA tool.

Bug 6161216

Stage patch job fails because some patches that uploaded to the software library and patch cache are corrupted during the upload.

Workaround   Delete patch from the software library and patch cache and retry uploading the patches.

Bug 6159772

When creating jobs using Enterprise Manager, the Time Zone Region drop down menu on the Job Schedule page will default to Pago Pago. If the default is not changed, the job will run in the Pago Pago time zone region, especially for repeating schedules.

Workaround   Select the appropriate time zone region from the list of time zones in the drop down menu.

Bug 6159713

Import of database is failing with `ORA-39126` error.

Workaround Select the `Overwrite Existing Datafiles` option during Enterprise Manager import.

Bug 6140573

Scheduling the purge job while configuring master sites for replication returns an error due to the wrong date format.

Workaround Change the date format specified in the `DBMS_DEFER_ SYS.SCHEDULE_PURGE` procedure to the corresponding locale and execute again.

Bug 6067548

While upgrading Enterprise Manager repository, the following errors are returned:

```
ORA-01403: no data foundError
ORA-06512: at "SYSMAN.JOB_INSERT_CRED_TYPE_DATA", line 52
ORA-04088: error during execution of trigger
'SYSMAN.JOB_INSERT_CRED_TYPE_DATA'
ORA-06512: at line 633
```

Workaround Click `Ignore` to continue.

Bug 5946279

On Internet Explorer, "Patch Prerequisites" interview wizard for the "Oracle Patch Prerequisite Checker" Deployment Procedure fails to successfully select Target and always returns an empty selection.

Workaround Retry with a later version of the browser or with another browser such as Mozilla Firefox v1.5.

Bug 5870061

You cannot create Materialized View group containing objects which are not owned by the Materialized View Administrator on Database Control.

Workaround None.

Bug 5592433

`storage_report_metrics.pl` may consume 100% of the CPU.

Workaround Rename `storage_report_metrics.pl` located in the `$ORACLE_ HOME/sysman/admin/scripts` directory.

Bug 4744069

When cloning Database Oracle Home using 11.1 (10.1/10.2) Database Control, you need to update the exclude file list. This file list specifies files that need not be included when the source Oracle Home is archived because these files are not required for the clone operation. The following files should not be included in the archive:

■ `sqlnet.ora`

- `tnsnames.ora`
- `listener.ora`
- `oratab`

Workaround   Update the exclude file list to specify the files that are not to be included in the archive.

38.17 Oracle Multimedia Known Bugs

Bug 6181300

Java proxy class method `OrdDicom.processCopy` to `OrdImage` does not `setProperties` of the `OrdImage` object.

Workaround: Applications need to call `OrdImage.setProperties()` method after a call to `OrdDicom.processCopy(String command, OrdImage dest)`.

38.18 Oracle OLAP Known Bugs

Bug 6140382

OLAP cannot be used in Oracle Shared Server mode.

Workaround: None.

Bug 6122166 and 6202997

Oracle BI Beans queries saved in 10g XML format cannot be run against an identical AW built in 11g.

Workaround: None.

Bug 6117650

Transportable tablespaces cannot be used with cube-organized materialized views.

Workaround: None.

Bug 6070531

Non-numeric data types cannot be loaded into measures of a cube.

Workaround: None.

Bug 6058877

Analytic workspaces in an instance upgraded to Oracle Database 11*g* Release 1 (11.1) in 10.2 compatibility mode may not have OLAP API access.

Workaround: None.

Bug 6040042 and 6040043

Oracle Data Pump cannot be used to export and import data from analytic workspaces.

Workaround: Use Oracle `EXPORT` and `IMPORT`.

38.19 Oracle Real Application Clusters Online Help Known Bugs

Bug 6192058

In non-English locales, clicking Help from the following pages displays an older version of online Help:

- Real Application Clusters Database Home page

- Performance page

- Top Activity page

- Cluster Cache Coherency page

- Instance Breakdown page

Workaround: None.

Bug 6191947

In non-English locales, clicking Help from the following pages displays the message `Topic Not Found`:

- Availability page

- Server page

- Schema page

- Data Movement page

- Software Support page

- Instance Breakdown for I/O page

Workaround: None.

38.20 Oracle SecureFiles Known Bugs

Bug 6316423

Executing `CREATE TABLE AS SELECT ... ENCRYPT` fails with internal errors.

Workaround: Execute `ALTER TABLE MODIFY ... ENCRYPT` after `CREATE TABLE AS SELECT` without the `ENCRYPT` option.

Bug 6191877

Executing `ALTER TABLE MOVE` with SecureFile LOBs encrypted fails with internal errors.

Workaround: Drop the table after exporting and re-create the table before importing.

38.21 Oracle SQL Developer Known Bugs

Bug 6275980

When `sqldeveloper.sh` is invoked from `$ORACLE_HOME/sqldeveloper`, there is a severe Java error seen on the prompt from where it is invoked. These errors are benign and can be safely ignored. This does not affect any functionality.

Workaround: None.

38.22 Oracle Ultra Search Known Bugs

Bug 5982938

Error SP2-1506 is appearing inside the ultrasearch.log file during custom database installation.

Workaround: Error SP2-1506, which is seen inside `ultrasearch.log`, can be ignored. It is not displayed as a popup. It is seen as text only inside the `cfgtoollogs/dbca/ultrasearch.log`. This does not affect any functionality.

38.23 Oracle Universal Installer Known Bugs

Bug 5908411

On hosts running SUSE Linux Enterprise Server 10 operating system, the prerequisite check "Checking Network Configuration requirements ..." fails with status as "Not executed".

Workaround: If the primary network interface of the host is configured with a static IP address, this error can be ignored by clicking on the box adjacent to the status column and installation can be resumed. Otherwise, the primary network interface of the host should be reconfigured with a static IP address before resuming the installation.

38.24 Oracle Warehouse Builder Known Bugs

Refer to "Open Bugs and Known Issues" in *Oracle Warehouse Builder Release Notes*.

38.25 Oracle XML DB Known Bugs

Bug 5964258

You cannot retrieve some nonschema-based XML data from XMLType table created with the `ALLOW NONSCHEMA` option.

Workaround: None.

Bug 5922702

Japanese characters become corrupt or unreadable on `ftp` (`ls` or `DIR`) when using the command prompt utilities with Windows XP Japanese Edition.

Workaround: None.

38.26 RMAN Known Bugs

Bug 3479963

Errors occur when backing up archived logs to a DVD writer on Windows.

Workaround: None.

Bug 2722635

The RMAN `CROSSCHECK` command can force the retrieval of files that have been migrated to HSM, because it opens the file to verify the contents of the first few blocks.

Workaround: Some HSM systems can be configured to leave a small portion of the file on disk. If that is possible, then this problem can be avoided by leaving the first 4M of every migrated file on disk. If that is not possible, then there is no workaround other than to not use the `CROSSCHECK` command.

Bug 2670671

Lack of statistics in RMAN catalog schema can lead to poor performance.

Workaround: Occasionally use the `ALTER USER ... COMPUTE STATISTICS` command to re-compute the statics for the RMAN catalog schema.

Bug 2353334

RMAN backups fail with internal errors when a nonstandard `db_block_size`, such as 6k, is used, and the tablespace that is being backed up has a standard block size, such as 8k or 16k.

Workaround: For disk backups, set `_db_file_direct_io_count` to the least common multiple of the `db_block_size` and the block size of the other tablespace. For tape backups, use the `BLKSIZE` RMAN channel parameter.

38.27 SQL Access Advisor Known Bugs

Bug 6238360

Do not use the `Show SQL` button on the `Recommendation` tab of the SQL Access Advisor. If you use this button, it will only show the SQL for the currently selected recommendations. If the selection of recommendations are changed later, the SQL will not be refreshed.

Workaround: None.

39 Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility

standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, seven days a week. For TTY support, call 800.446.2398.