Database Upgrade Guide

4 Post-Upgrade Tasks for Oracle Database

After performing the procedures for upgrading Oracle Database, you must complete required tasks and consider recommendations for the new release.

This chapter contains the following topics:

- How to Show the Current State of the Oracle Data Dictionary (#CHDFCAHG)
- About OPatch Commands After Upgrading Oracle Database (#CHDBHHGA)
- Required Tasks to Complete After Upgrading Oracle Database (#CEGBJCBA)
- Required Task After Oracle Grid Infrastructure Upgrades (#CEGCHFAC)
- Requirement for Role-Allocated Software Owners and Database Upgrade After Oracle ASM Upgrade (#CEGBGBII)
- Recommended and Best Practices to Complete After Upgrading Oracle Database (#CEGHGAIG)
- Recommended Tasks After Upgrading an Oracle RAC Database (#CEGGEECD)
- Recommended Tasks After Upgrading Oracle ASM (#CEGBDIHI)
- Recommended Tasks After Upgrading Oracle Database Express Edition (#CEGEJIJG)
- Optionally Update Oracle Application Express Packaged Applications (#CHDIJCFE)
- Tasks to Complete Only After Manually Upgrading Oracle Database (#CEGGHCAD)

4.1 How to Show the Current State of the Oracle Data Dictionary

You can collect upgrade and migration diagnostic information about the current state of the data dictionary by running the `dbupgdiag.sql` script. The script can be run in SQL*Plus both before the upgrade on the source database and after the upgrade on the upgraded database as SYS user.

> **See Also:**
>
> Note 556610.1 Script to Collect DB Upgrade/Migrate Diagnostic Information (dbupgdiag.sql) on My Oracle Support at at `http://support.oracle.com` (`http://support.oracle.com`)

To show the current state of the dictionary, execute a SQL query similar to the following example:

```
SQL> spool /tmp/regInvalid.out SQL> set echo on -- query registry SQL> set lines 80
pages 100 SQL> select substr(comp_id,1,15) comp_id,substr(comp_name,1,30)
comp_name,substr(version,1,10) version,status from dba_registry order by modified;
```

To query invalid objects, execute a SQL query similar to:

```
SQL> select substr(owner,1,12) owner,substr(object_name,1,30)
object,substr(object_type,1,30) type, status from dba_objects where status <>
'VALID'order by owner, type; SQL> spool off SQL> set echo off
```

4.2 About OPatch Commands After Upgrading Oracle Database

After you upgrade Oracle Database, you must run OPatch commands from the new Oracle home. For example, run the `lsinventory` command from the new Oracle home in order to list an accurate and complete inventory of what is currently installed on the system.

> **See Also:**
>
> "Appendix A" in *Oracle OPatch User's Guide for Windows and UNIX* (http://www.oracle.com/pls/topic/lookup?ctx=E50529-01&id=OPTCH)for OPatch syntax and commands

4.3 Required Tasks to Complete After Upgrading Oracle Database

After you upgrade Oracle Database, regardless of whether you perform the upgrade manually, or upgrade by using Database Upgrade Assistant (DBUA), you must complete any required tasks that are specified for your environment.

- Set Environment Variables on Linux and UNIX Systems After Manual Upgrades (#CEGCBIIE)
- Upgrade the Recovery Catalog After Upgrading Oracle Database (#CEGDBEBF)
- Upgrade the Time Zone File Version After Upgrading Oracle Database (#CEGBGBDA)
- Upgrade Statistics Tables Created by the DBMS_STATS Package After Upgrading Oracle Database (#CEGBGAFB)
- Upgrade Externally Authenticated SSL Users After Upgrading Oracle Database (#CEGCJHDI)
- Configure the FTP and HTTP Ports and HTTP Authentication for Oracle XML DB (#CHDGBIFJ)
- Install Oracle Text Supplied Knowledge Bases After Upgrading Oracle Database (#CEGBIBCF)
- Update Your Oracle Application Express Configuration After Upgrading Oracle Database (#CEGECAHJ)
- Configure Access Control Lists (ACLs) to External Network Services (#CEGDGAHJ)
- Enable Oracle Database Vault After Upgrading Oracle Database (#CEGDGAIC)

- Check for the SQLNET.ALLOWED_LOGON_VERSION Parameter Behavior (#CHDCFAHG)

4.3.1 Set Environment Variables on Linux and UNIX Systems After Manual Upgrades

If your operating system is Linux or UNIX, and if you performed a manual upgrade of Oracle Database, then you must ensure that certain environment variables point to the directories of the new Oracle Database release. Additionally, if you are upgrading a cluster database, then perform these checks on all nodes on which the cluster database has instances configured.

Confirm that the following environment variables point to the directories of the new Oracle home:

- `ORACLE_HOME`
- `PATH`

> **Note:**
>
> DBUA automatically makes necessary changes to Oracle environment variables.

> **See Also:**
>
> - *Oracle Database Administrator's Guide* (../ADMIN/create.htm#ADMIN12480)for information about setting environment variables for the database
> - *Oracle Database Installation Guide* (http://www.oracle.com/pls/topic/lookup?ctx=E5052901&id=GINST) for your operating system for information about setting other important environment variables

4.3.2 Set oratab and Scripts to Point to the New Oracle Location After Upgrading Oracle Database

After you upgrade Oracle Database to the new release, you must ensure that your `oratab` file and any client scripts that set the value of *`ORACLE_HOME`* point to the new Oracle home that is created for the new Oracle Database 12*c* release. Although DBUA automatically points `oratab` to the new Oracle home, client scripts must be checked no matter which method you use to upgrade.

> **See Also:**
>
> *Oracle Database Administrator's Guide* (../ADMIN/dba.htm#ADMIN12475)for information about setting operating system environment variables

4.3.3 Enable the New Extended Data Type Capability

Oracle Database 12*c* introduces `MAX_STRING_SIZE` to control the maximum size of `VARCHAR2`, `NVARCHAR2`, and `RAW` data types in SQL. Setting `MAX_STRING_SIZE = EXTENDED` enables the 32767 byte limit introduced in Oracle Database 12*c*. The `COMPATIBLE` initialization parameter must be set to `12.0.0.0` or higher in order to be able to set `MAX_STRING_SIZE = EXTENDED`.

Enabling a system to take advantage of the new extended data types requires specific upgrade actions, as documented in the *Oracle Database Reference* (../REFRN/GUID-D424D23B-0933-425F-BC69-9C0E6724693C.htm#REFRN10321). You can change the value of `MAX_STRING_SIZE` from `STANDARD` to `EXTENDED`.

However, you cannot change the value of `MAX_STRING_SIZE` from `EXTENDED` to `STANDARD`. By setting `MAX_STRING_SIZE = EXTENDED`, you are taking an explicit action that could introduce application incompatibility in your database.

> **See Also:**
>
> *Oracle Database Reference* (../REFRN/GUID-D424D23B-0933-425F-BC69-9C0E6724693C.htm#REFRN10321) for complete information about `MAX_STRING_SIZE`, including recommendations and procedures

4.3.4 Adjust Minimum and Maximum for Parallel Execution Servers

In Oracle Database 12*c* the default for `PARALLEL_MIN_SERVERS` has been changed from `0` to a value depending on your hardware platform to accommodate sufficient minimal support for parallel execution. If the new default setting is too high for your environment, then adjust the setting for your requirements.The default for `PARALLEL_MAX_SERVERS` has not changed, and, therefore, if you have not changed the default in your old environment, no actions are needed.

> **See Also:**
>
> *Oracle Database Reference* (../REFRN/GUID-1D7EC131-7B5B-40E5-A0F8-ABC7B4C5B0E8.htm#REFRN10160) for information about `PARALLEL_MIN_SERVERS`

4.3.5 Upgrade the Recovery Catalog After Upgrading Oracle Database

If you use a version of the recovery catalog schema that is older than that required by the RMAN client, then you must upgrade it. For complete information about upgrading the recovery catalog and the `UPGRADE CATALOG` command, see *Oracle Database Backup and Recovery User's Guide* (../BRADV/rcmcatdb.htm#BRADV188).

> **See Also:**
>
> *Oracle Database Backup and Recovery User's Guide* (../BRADV/rcmcatdb.htm#BRADV8015) for information on managing an RMAN recovery catalog

4.3.6 Upgrade the Time Zone File Version After Upgrading Oracle Database

If the Pre-Upgrade Information Tool instructed you to upgrade the time zone files after completing the database upgrade, then use the `DBMS_DST` PL/SQL package to upgrade the time zone file.

Oracle Database supplies multiple versions of time zone files, and there are two types of file associated with each one: a large file, which contains all the time zones defined in the database, and a small file, which contains only the most commonly used time zones. The large versions are designated as `timezlrg_`*`version_number`*`.dat`, while the small versions are designated as `timezone_`*`version_number`*`.dat`. The files are located in the `oracore/zoneinfo` subdirectory under the Oracle Database home directory.

> **See Also:**
>
> - *Oracle Database Globalization Support Guide* (../NLSPG/ch4datetime.htm#NLSPG261) and follow the procedure in "Steps to Upgrade Time Zone File and Timestamp with Time Zone Data"

- Note ID 1509653.1 "Updating the RDBMS DST version in 12*c* Release 1 (12.1.0.1 and up) using DBMS_DST" on My Oracle Support at http://support.oracle.com (http://support.oracle.com)
- "About Oracle Database Warnings for TIMESTAMP WITH TIME ZONE Data Type" (preup.htm#BABJBJBH)

4.3.7 Upgrade Statistics Tables Created by the DBMS_STATS Package After Upgrading Oracle Database

If you created statistics tables using the DBMS_STATS.CREATE_STAT_TABLE procedure, then upgrade these tables by running the following procedure:

```
EXECUTE DBMS_STATS.UPGRADE_STAT_TABLE('green', 'stat_table');
```

In the example, green is the owner of the statistics table and STAT_TABLE is the name of the statistics table. Perform this procedure for each statistics table.

See Also:

Oracle Database PL/SQL Packages and Types Reference (../ARPLS/d_stats.htm#ARPLS059)for information about the DBMS_STATS package

4.3.8 Upgrade Externally Authenticated SSL Users After Upgrading Oracle Database

If you are upgrading from Oracle9*i* Release 2 (9.2) or Oracle Database 10*g* Release 1 (10.1), and you are using externally authenticated SSL users, then you must run the SSL external users conversion (extusrupgrade) script to upgrade those users. The script has the following syntax:

```
ORACLE_HOME/rdbms/bin/extusrupgrade --dbconnectstring host_name:port_no:sid --dbuser
<db admin> --dbuserpassword password -a
```

Note:

If you are upgrading from Oracle Database 10*g* Release 2 (10.2) or later, then you are not required to run the extusrupgrade script.

See Also:

Oracle Database Enterprise User Security Administrator's Guide (../DBIMI/appb.htm#DBIMI348)for more information on the extusrupgrade script

4.3.9 Configure the FTP and HTTP Ports and HTTP Authentication for Oracle XML DB

For Oracle Database 12*c*, Database Creation Assistant (DBCA) does not configure ports for Oracle XML DB. You should also configure the authentication for HTTP for accessing Oracle XML DB Repository to take advantage of improved security features.

Starting with Oracle Database 12*c*, Oracle has enhanced database security by providing support for digest authentication. Digest authentication is an industry standard protocol commonly used with the HTTP protocol, and is supported by most HTTP clients. Digest authentication ensures that passwords are always transmitted

in a secure manner, even when an encrypted (HTTPS) connection is not in use. Support for digest authentication enables organizations to deploy applications that leverage the Oracle XML DB HTTP without having to worry about passwords being compromised. Digest authentication support in Oracle XML DB also ensures that the Oracle XML DB HTTP server remains compatible with Microsoft Web Folders WebDAV clients.

> **See Also:**
>
> *Oracle XML DB Developer's Guide* (../ADXDB/xdb22pro.htm#ADXDB2540)for information on configuring and managing authentication mechanisms for HTTP

After installing or upgrading for the new release, you must manually configure the FTP and HTTP ports for Oracle XML DB as follows:

1. Use `DBMS_XDB_CONFIG.setHTTPPort(`*`HTTP port number`*`)` to set the HTTP port for Oracle XML DB.

   ```
   SQL> exec DBMS_XDB_CONFIG.setHTTPPort(port_number);
   ```

2. Use `DBMS_XDB_CONFIG.setFTPPort(`*`FTP port number`*`)` to set the FTP port for Oracle XML DB.

   ```
   SQL> exec DBMS_XDB_CONFIG.setFTPPort(port_number);
   ```

   > **Note:**
   >
   > You can query the port numbers to use for FTP and HTTP in the procedure by using `DBMS_XDB_CONFIG.getFTPPort` and `DBMS_XDB_CONFIG.getHTTPPort` respectively.

3. To see all the used port numbers, you can use `DBMS_XDB_CONFIG.usedport`.

> **See Also:**
>
> *Oracle XML DB Developer's Guide* (../ADXDB/xdb22pro.htm#ADXDB2500)for complete information about accessing the Oracle XML DB Repository data using FTP and HTTP(S)/WebDAV protocols

4.3.10 Install Oracle Text Supplied Knowledge Bases After Upgrading Oracle Database

The Oracle Text-supplied knowledge bases are part of the companion products for Oracle Database 12*c* and are not immediately available after an upgrade to Oracle Database 12*c*. Any Oracle Text features dependent on the supplied knowledge bases which were available before the upgrade do not function after the upgrade. To re-enable such features, you must install the Oracle Text supplied knowledge bases from the installation media.

After an upgrade, all user extensions to the Oracle Text supplied knowledge bases must be regenerated. These changes affect all databases installed in the given Oracle home.

> **See Also:**
>
> - *Oracle Text Application Developer's Guide* (../CCAPP/GUID-05C24323-568D-4952-9358-7C98D68B19BF.htm#CCAPP0900) for information about Oracle Text-supplied knowledge bases
> - The postinstallation tasks section of your platform-specific *Oracle Database Installation Guide* (http://www.oracle.com/pls/topic/lookup?ctx=E5052901&id=GINST) for companion products

4.3.11 Update Your Oracle Application Express Configuration After Upgrading Oracle Database

If your database originally included Oracle Application Express release 3.2 or later, then there is no additional configuration necessary after upgrading to Oracle Database 12*c*. However, if Oracle Application Express is in the registry and Oracle Application Express will be upgraded, then you should set the `open_cursors` parameter to a minimum of 200.

If your database was not an Oracle Express Edition database, but contained an earlier release of Oracle Application Express, then the latest release is automatically installed during the upgrade. You must complete a series of postinstallation steps to configure Application Express for use with the new Oracle Database 12*c*.

> **See Also:**
>
> *Oracle Application Express Installation Guide* (../HTMIG/db_install.htm#HTMIG203)for postinstallation tasks for Oracle Application Express

If your database is an Oracle Express Edition database, then it contains an earlier release of Oracle Application Express, which is tailored for the Oracle Express Edition environment. Review the Oracle document describing the differences between Oracle Express Edition and Oracle Application Express at the following URL:

`http://www.oracle.com/technetwork/developer-tools/apex/overview/index.html`
`(http://www.oracle.com/technetwork/developer-tools/apex/overview/index.html)`

4.3.12 Configure Access Control Lists (ACLs) to External Network Services

Oracle Database 12*c* includes fine-grained access control to the `UTL_TCP`, `UTL_SMTP`, `UTL_MAIL`, `UTL_HTTP`, or `UTL_INADDR` packages. If you have applications that use these packages, then after upgrading Oracle Database you must configure network *access control lists* (ACLs) in the database before these packages can work as they did in earlier releases. Without the ACLs, your applications may fail with the error "ORA-24247: network access denied by access control list (ACL)."

> **See Also:**
>
> *Oracle Database Security Guide* (../DBSEG/fine_grained_access.htm#DBSEG40012)for more complicated situations, such as connecting some users to host A and other users to host B

4.3.13 Enable Oracle Database Vault After Upgrading Oracle Database

If you use Oracle Database Vault (DV), then you were instructed to disable it before upgrading your database. You must now enable Oracle Database Vault.

To start Oracle DV enforcement in the upgraded database, enable DV using the procedure `dvsys.dbms_macadm.enable_dv()`. A user with the `DV_OWNER` or `DV_ADMIN` role is the only one who can execute this procedure. For the procedure to take effect, the database instance needs to be restarted.

> **See Also:**
>
> - "Requirement for Upgrading Oracle Databases That Use Oracle Database Vault" (preup.htm#BABIHIGB)

- The appendix about "Disabling and Enabling Database Vault" in *Oracle Database Vault Administrator's Guide* (../DVADM/dvdisabl.htm#DVADM012)
- The appendix about "Post-installation Database Vault Procedures" in *Oracle Database Vault Administrator's Guide* (../DVADM/getting_started.htm#DVADM30031)

4.3.14 Check for the SQLNET.ALLOWED_LOGON_VERSION Parameter Behavior

Starting with Oracle Database 12*c*, the default value for the `SQLNET.ALLOWED_LOGON_VERSION` parameter has changed from 8 to 11. The use of this parameter has been deprecated, and it is now replaced with the `SQLNET.ALLOWED_LOGON_VERSION_SERVER` and `SQLNET.ALLOWED_LOGON_VERSION_CLIENT` parameters. If you have not explicitly set the `SQLNET.ALLOWED_LOGON_VERSION_SERVER` parameter in the upgraded database, then connections from clients earlier than release 10*g* will fail with the error ORA-28040: No matching authentication protocol. For better security, check the password verifiers of your database users, and then configure the database to use the correct password verifier by setting the `SQLNET.ALLOWED_LOGON_VERSION_SERVER` and `SQLNET.ALLOWED_LOGON_VERSION_CLIENT` parameters.

If you have password-protected roles (secure roles) in your existing database and if you upgrade to Oracle Database 12*c* with the default `SQLNET.ALLOWED_LOGON_VERSION_SERVER` setting of 11, because those secure roles only have release 10*g* verifiers, the password for each secure role must be reset by the administrator so that the secure roles will remain usable after the upgrade.

See Also:

- *Oracle Database Security Guide* (../DBSEG/authentication.htm#DBSEG30324)for information about ensuring against password security threats
- *Oracle Database Security Guide* (../DBSEG/authentication.htm#DBSEG3225)for information about setting the password versions of users
- "Deprecation of SQLNET.ALLOWED_LOGON_VERSION Parameter" (deprecated.htm#BABEDDGA)

4.4 Required Task After Oracle Grid Infrastructure Upgrades

After upgrading, you should confirm that your environment variable settings are correct. See "Using Environment Variables for Grid Infrastructure Installations." (#CEGJABBC) Oracle ASM is included as part of an Oracle Grid Infrastructure installation. If you upgrade Oracle Clusterware and Oracle ASM for a cluster, then Oracle Clusterware and Oracle ASM are both located in the same home, which is referred to as *Grid home*. You can have one installation owner that owns all Oracle software installations, or you can use role-allocated owners, in which case you use a separate software owner for the Grid Infrastructure installation, and separate software owners for one or more Oracle Database installations.

See Also:

Oracle Grid Infrastructure Installation Guide (http://www.oracle.com/pls/topic/lookup?ctx=E5052901&id=CWGEN) for your platform for more information about role-allocated installation owners

4.4.1 Using Environment Variables for Grid Infrastructure Installations

If your operating system is Linux or UNIX, then confirm that your environment variable settings are correct after performing an upgrade.

If you use a single Oracle installation owner for all installations, then be aware that you should change environment variables such as `ORACLE_HOME` either to an Oracle Database home, or to the Grid home, depending on whether you are administering an Oracle Database instance as part of database administration, or administering an Oracle ASM instance as part of storage administration.

If you use role-allocated Oracle installation owners, so that you have a separate owner for the Oracle Grid Infrastructure (Oracle Clusterware and Oracle ASM) software, then set the following environment variables for the Grid Infrastructure installation owner so that they point to the directories of the Oracle ASM home in the Grid home:

- `ORACLE_HOME`
- `PATH`

Also, check that your `oratab` file and any client scripts for Oracle ASM that set the value of `ORACLE_HOME` point to the Oracle ASM home in the Grid home.

> **Note:**
>
> If you are upgrading a clustered Oracle ASM installation to an Oracle Grid Infrastructure for a cluster installation, then perform these checks on all cluster member nodes. DBUA automatically points `oratab` to the new Oracle home. Client scripts must be checked no matter how you upgrade.

> **See Also:**
>
> - Your operating system-specific *Oracle Database Installation Guide* (http://www.oracle.com/pls/topic/lookup?ctx=E50529-01&id=GINST) for information about setting other important environment variables on your operating system
> - *Oracle Grid Infrastructure Installation Guide* (http://www.oracle.com/pls/topic/lookup?ctx=E5052901&id=CWGEN) or *Oracle Database Installation Guide* (http://www.oracle.com/pls/topic/lookup?ctx=E5052901&id=GINST) for your platform
> - *Oracle Automatic Storage Management Administrator's Guide* (../OSTMG/GUID-DEF14BF6-30C4-4B52-969D-97158063F612.htm#OSTMG94317) for information about upgrading an Oracle ASM instance

4.5 Requirement for Role-Allocated Software Owners and Database Upgrade After Oracle ASM Upgrade

If you separate the operating system user ownership of the Oracle Grid Infrastructure binaries and the Oracle Database installation owners of one or more databases, then you must migrate the operating system user of an upgraded Oracle ASM or database home. For example, if you are migrating from one software binary owner

(such as `oracle`) to multiple role-allocated software owner user accounts (such as `grid`, `oracle1`, `oracle2`), then change the owner of the existing Oracle ASM installation owner to the installation owner that you plan to use for the Oracle Grid Infrastructure installation.

There are three scenarios to consider as follows:

- Keeping the Existing User as the Oracle ASM Operating System User (#CEGBFJGC)
- Changing the Operating System User for Single-Instance Oracle ASM (#CEGDEAGC)
- Changing the Operating System User for an Oracle RAC Database (#CEGCFFJC)

> **See Also:**
>
> *Oracle Automatic Storage Management Administrator's Guide* (../OSTMG/GUID-FBB5AA72-5208-48E1-BD8D-0FD4C6876F34.htm#OSTMG02700)for information on making an Oracle ASM disk group compatible with new releases, and for additional information about Oracle ASM upgrades

4.5.1 Keeping the Existing User as the Oracle ASM Operating System User

If you are using the same operating system user for your Oracle Grid Infrastructure installation that you used for your existing Oracle ASM installation, then run Oracle Universal Installer (OUI) to perform a Grid Infrastructure installation, and select the upgrade option. OUI automatically upgrades your existing Oracle ASM installation from the earlier release to Oracle Database 12*c* in the Grid home.

4.5.2 Changing the Operating System User for Single-Instance Oracle ASM

Consider your earlier release Oracle ASM installation is installed in Oracle home 4 (`OH4`) and currently running `oracle` as the operating system user, and you want to change the Oracle ASM operating system user to `grid`. This is useful if you have two databases using Oracle ASM, and you had installed Oracle ASM with an installation owner that is identical to the owner of the existing databases, and you want to change the operating system installation owner of Oracle ASM to enable separate databases to run as separate operating system users, where neither Oracle Database installation owner has Oracle Grid Infrastructure binary ownership.

4.5.3 Changing the Operating System User for an Oracle RAC Database

There may be scenarios where you must change the operating system user for an Oracle RAC database. For example, if your earlier release database is installed in Oracle home 4 (`OH4`) and currently running `oracle` as the operating system user, then you should consider changing the Oracle ASM operating system user to `grid`. Changing the operating system user of Oracle ASM enables separate databases to run as separate operating system users, where no Oracle Database installation owner has Grid Infrastructure binary ownership.

> **See Also:**
>
> *Oracle Grid Infrastructure Installation Guide* (http://www.oracle.com/pls/topic/lookup?ctx=E5052901&id=CWGEN10001)for the procedures to change the operating system user for an Oracle RAC database with Grid Infrastructure and Oracle ASM

4.6 Recommended and Best Practices to Complete After Upgrading Oracle Database

After you have upgraded Oracle Database, there are tasks Oracle recommends that you complete. These tasks represent good practices for updating Oracle Database, and are recommended regardless of whether you performed the upgrade manually or by using DBUA.

- Back Up the Database (#CEGHJAGH)
- Run the postupgrade_fixups.sql Script (#CHDJACCG)
- Gather Fixed Objects Statistics with DBMS_STATS (#CHDDADDD)
- Reset Passwords to Enforce Case-Sensitivity (#CEGCIEGH)
- Understand Changes with Oracle Grid Infrastructure (#CEGCEBDE)
- Understand Oracle ASM and Oracle Grid Infrastructure Installation and Upgrade (#CEGEDDAE)
- Add New Features as Appropriate (#CEGHDJEF)
- Develop New Administrative Procedures as Needed (#CEGFIHCI)
- Set Threshold Values for Tablespace Alerts (#CEGHHDFE)
- Migrate From Rollback Segments to Automatic Undo Mode (#CEGHGBJE)
- Configure Oracle Data Guard Broker (#CEGCDBGG)
- Migrate Tables from the LONG Data Type to the LOB Data Type (#CEGFFJGF)
- Migrate Your Upgraded Oracle Databases to Use Unified Auditing (#CHDEFHGA)
- Test the Upgraded Production Oracle Database (#CEGGFBJI)

4.6.1 Back Up the Database

Make sure you perform a full backup of the production database. Although this step is not required, Oracle strongly recommends that you back up your production database.

> **See Also:**
>
> *Oracle Database Backup and Recovery User's Guide* (../BRADV/rcmbckba.htm#BRADV8003)for details about backing up a database with RMAN

4.6.2 Run the postupgrade_fixups.sql Script

Although DBUA runs the `postupgrade_fixups.sql` script as part of completing the upgrade process, you can run it any time after upgrading. The `postupgrade_fixups.sql` script generates three categories of information for your upgraded database: general warnings, errors, and informational recommendations.

Run this script any time after completing an upgrade with DBUA or manually. If *`Oracle_Base`* is defined, then the generated scripts and log files are created in *`Oracle_Base`*`/cfgtoollogs/` of the original database from which you ran the upgrade. If *`Oracle_Base`* is not defined, then the generated scripts and log files are created in *`ORACLE_HOME`*`/cfgtoollogs/` of the database from which you ran the upgrade.

Set the system to spool results to a log file so you can read the output. Do not, however, spool to the `admin` directory. Run the script from the location of the database from which you ran the upgrade (not the new upgraded location):

```
SQL> SPOOL postupgrade.log
```

Turn off the spooling of script results to the log file.

```
SQL> SPOOL OFF
```

> **Note:**
>
> If you move either a PDB or any other stand-alone database from server A to server B, you must copy the `postupgrade_fixups.sql` script to the new location to execute it post-upgrade in the new environment.

4.6.3 Gather Fixed Objects Statistics with DBMS_STATS

A few days after upgrading Oracle Database, a best practice is to gather fixed objects statistics with the `DBMS_STATS.GATHER_FIXED_OBJECTS_STATS` PL/SQL procedure. This can have a positive impact on overall database performance. `DBMS_STATS.GATHER_FIXED_OBJECTS_STATS` also displays a recommendation to remove all hidden or underscore parameters and events from `init.ora/spfile`.

Because of the transient nature of the x$ tables, it is important that you gather fixed objects statistics when there is a representative workload on the system. This may not always be feasible on large systems due to additional resources needed to gather the statistics. If you cannot do this during peak load, then you should do it after the system has warmed up and the key types of fixed object tables have been populated.

To gather statistics for fixed objects, run the following PL/SQL procedure:

```
SQL> execute dbms_stats.gather_fixed_objects_stats;
```

> **See Also:**
>
> *Oracle Database PL/SQL Packages and Types Reference* (../ARPLS/d_stats.htm#ARPLS68573)for more information about using the `GATHER_FIXED_OBJECTS_STATS` procedure

4.6.4 Reset Passwords to Enforce Case-Sensitivity

You can enforce case sensitivity for passwords. For example, the password `hPP5620qr` fails if it is entered as `hpp5620QR` or `hPp5620Qr`.

If you must reset the passwords of existing users during the database upgrade procedure, then for existing databases each user password must be reset with an `ALTER USER` statement. For new databases created after the upgrade, there are no additional tasks or management requirements.

To take advantage of enforced case-sensitive passwords for releases earlier than 11.1.0.7, you must reset the passwords of existing users during the database upgrade procedure. In this case, for upgraded databases, you can run the `DBMS_VERIFIER.EXPIRE_ACCOUNTS_WITHOUT_LATEST_VERIFIER` procedure, which forces users whose accounts do not yet have the latest verifier to change their passwords the next time they log in. The server can then generate the latest verifier for their account. For new databases, there are no additional tasks or management requirements.

For `SYSDBA` and `SYSOPER` users, you can generate a new `ORAPWD` file using the new command line switch `ignorecase`.

Note:

- If the default security settings for Oracle Database 12*c* are in place, then passwords must be at least eight characters, and passwords such as `welcome` and `oracle` are not allowed. See *Oracle Database Security Guide* (../DBSEG/guidelines.htm#DBSEG10005)for more information on password strength.

- The `IGNORECASE` parameter is deprecated in this release. Oracle recommends not using this parameter.

See Also:

Oracle Database Security Guide (../DBSEG/authentication.htm#DBSEG3225)for more information on enabling password case sensitivity

4.6.5 Understand Changes with Oracle Grid Infrastructure

Oracle Clusterware and Oracle ASM are both part of an Oracle Grid Infrastructure installation.

If Oracle Grid Infrastructure is installed for a single server, then it is deployed as an Oracle Restart installation with Oracle ASM. If Oracle Grid Infrastructure is installed for a cluster, then it is deployed as an Oracle Clusterware installation with Oracle ASM.

Oracle Restart enhances the availability of Oracle Database in a single-instance environment. If you install Oracle Restart, and there is a temporary failure of any part of the Oracle Database software stack, including the database, listener, and Oracle ASM instance, Oracle Restart automatically restarts the failed component. In addition, Oracle Restart starts all these components when the database host computer is restarted. The components are started in the proper order, taking into consideration the dependencies among components.

Oracle Clusterware is portable cluster software that enables clustering of single servers so that they cooperate as a single system. Oracle Clusterware also provides the required infrastructure for Oracle RAC. In addition, Oracle Clusterware enables the protection of any Oracle application or any other application within a cluster. In any case Oracle Clusterware is the intelligence in those systems that ensures required cooperation between the cluster nodes.

See Also:

Oracle Grid Infrastructure Installation Guide (http://www.oracle.com/pls/topic/lookup?ctx=E5052901&id=CWGEN10001)for more information and procedures

4.6.6 Understand Oracle ASM and Oracle Grid Infrastructure Installation and Upgrade

In earlier releases, Oracle ASM was installed as part of the Oracle Database installation. Starting with Oracle Database release 11.2, Oracle ASM is installed when you install the Grid Infrastructure components. Oracle ASM shares an Oracle home with Oracle Clusterware when it is installed in a cluster such as with Oracle RAC or with Oracle Restart on a standalone server.

See Also:

Oracle Grid Infrastructure Installation Guide (http://www.oracle.com/pls/topic/lookup?ctx=E5052901&id=CWGEN10001)for more information and procedures

4.6.7 Add New Features as Appropriate

The *Oracle Database New Features Guide* (../NEWFT/toc.htm) describes many of the new features available in the new Oracle Database 12*c* release. Determine which of these new features can benefit the database and applications. You can then develop a plan for using these features.

It is not necessary to make any immediate changes to begin using your new Oracle Database software. You might prefer to introduce these enhancements into your database and corresponding applications gradually.

Chapter 5, "Upgrading Applications After Upgrading Oracle Database" (app.htm#BABHJHEH) describes ways to enhance your applications so that you can take advantage of the features of the new Oracle Database 12*c* release. However, before you implement new features, test your applications and successfully run them with the upgraded database.

4.6.8 Develop New Administrative Procedures as Needed

After familiarizing yourself with the features of the new Oracle Database 12*c* release, review your database administration scripts and procedures to determine whether any changes are necessary.

Coordinate your changes to the database with the changes that are necessary for each application. For example, by enabling integrity constraints in the database, you might be able to remove some data checking from your applications.

4.6.9 Set Threshold Values for Tablespace Alerts

An upgraded Oracle Database 12*c* database has the Tablespace Alerts disabled (the thresholds are set to null). Tablespaces in the database that are candidates for monitoring must be identified and the appropriate threshold values set.

The default threshold values for a newly created Oracle Database 12*c* database are:

- 85% full warning
- 97% full critical

4.6.10 Migrate From Rollback Segments to Automatic Undo Mode

If your database is earlier than Oracle Database 11*g*, then you must migrate the database that is being upgraded from using rollback segments (manual undo management) to automatic undo management.

Automatic undo management is the default undo space management mode. The `UNDO_MANAGEMENT` initialization parameter specifies which undo space management mode the system should use, as follows:

- If `UNDO_MANAGEMENT=AUTO` (or if `UNDO_MANAGEMENT` is not set), then the database instance starts in automatic undo management mode.

  A null `UNDO_MANAGEMENT` initialization parameter defaults to automatic undo management mode in Oracle Database 11*g* Release 1 (11.1), but it defaults to manual undo management mode in earlier releases. You must therefore use caution when upgrading 10.2 or 11.1 releases to Oracle Database 12*c*.

- If `UNDO_MANAGEMENT=MANUAL`, then undo space is allocated externally as rollback segments.

To migrate to automatic undo management, perform the following steps:

1. Set `UNDO_MANAGEMENT=MANUAL`.

2. Start the instance again and run through a standard business cycle to obtain a representative workload. Doing this to assess the workload and compute the size of the undo tablespace required for automatic undo management.

3. After the standard business cycle completes, run the following function to collect the undo tablespace size and help with the sizing of the undo tablespace (DBA privileges are required to run this function):

   ```
   DECLARE utbsiz_in_MB NUMBER; BEGIN utbsiz_in_MB := DBMS_UNDO_ADV.RBU_MIGRATION;
   end; /
   ```

   This function runs a PL/SQL procedure that provides information on how to size your new undo tablespace based on the configuration and usage of the rollback segments in your system. The function returns the sizing information directly.

4. Create an undo tablespace of the required size and turn on the automatic undo management by setting `UNDO_MANAGEMENT=AUTO` or by removing the parameter.

5. For Oracle RAC configurations, repeat these steps on all instances.

4.6.11 Configure Oracle Data Guard Broker

The value of `DGConnectIdentifier` is used for all Data Guard network traffic, all of the time. If you are upgrading an Oracle Database release 10*g* configuration, which requires you to first upgrade to Oracle Database 11*g*, the value that exists for `InitialConnectIdentifier` is retained as the new value for `DGConnectIdentifier` for the database. When upgrading an Oracle RAC database, the database administrator must ensure that the value for the `InitialConnectIdentifier` property reaches all instances.

4.6.12 Migrate Tables from the LONG Data Type to the LOB Data Type

The `LOB` data types (`BFILE`, `BLOB`, `CLOB`, and `NCLOB`) can provide many advantages over `LONG` data types. You can use the `ALTER TABLE` statement to change the data type of a `LONG` column to `CLOB` and that of a `LONG RAW` column to `BLOB`.

In the following example, the `LONG` column named `long_col` in table `long_tab` is changed to data type `CLOB`:

```
SQL> ALTER TABLE Long_tab MODIFY ( long_col CLOB );
```

After using this method to change `LONG` columns to LOBs, all the existing constraints and triggers on the table are still usable. However, all the indexes, including Domain indexes and Functional indexes, on all columns of the table become unusable and must be rebuilt using an `ALTER INDEX...REBUILD` statement. Also, the Domain indexes on the `LONG` column must be dropped before changing the `LONG` column to a LOB.

> **See Also:**
>
> *Oracle Database SecureFiles and Large Objects Developer's Guide* (../ADLOB/adlob_intro.htm#ADLOB001)for information about modifying applications to use LOB data

4.6.13 Migrate Your Upgraded Oracle Databases to Use Unified Auditing

In unified auditing, all Oracle Database audit trails (`SYS.AUD$` for the database audit trail, `SYS.FGA_LOG$` for fine-grained auditing, `DVYS.AUDIT_TRAIL$` for Database Vault, and so on) are combined into one single audit trail, which you can view by querying the `UNIFIED_AUDIT_TRAIL` data dictionary view for single-instance installations and `GV$UNIFIED_AUDIT_TRAIL` for Oracle Real Application Clusters environments. If you want to use the full, pure unified auditing facility, then you must manually migrate to it as described in "Migrating to Unified Auditing for Oracle Database" (#CHDFBBAG).

> **See Also:**
>
> *Oracle Database Security Guide* (../DBSEG/audit_changes.htm#DBSEG341)for information about how the audit features have changed for this release

This section contains the following topics:

- About the Unified Auditing Migration Process for Oracle Database (#CHDCEIBH)
- Migrating to Unified Auditing for Oracle Database (#CHDFBBAG)
- Managing Earlier Audit Records After You Migrate to Unified Auditing (#CHDHHIBB)
- Removing the Unified Auditing Functionality (#CHDJEEHF)
- Documentation References if You Choose Not to Use Unified Auditing (#CHDFFFHJ)

4.6.13.1 About the Unified Auditing Migration Process for Oracle Database

By default, unified auditing is not enabled for upgraded databases. If you have upgraded from an earlier release to Oracle Database 12*c*, then your database uses the same auditing functionality that was used in the earlier release. For newly created databases, the mixed-mode method of unified auditing is enabled by default. After you complete the migration to unified auditing, traditional auditing is disabled and the new audit records write to the unified audit trail.

To enable and configure the audit policies and how they are used, choose one method as follows:

- Use the pure unified audit facility.

  Follow the procedure described in "Migrating to Unified Auditing for Oracle Database" (#CHDFBBAG)to use the pure unified auditing facility. Once the procedure for migrating to unified auditing is complete, you can create and enable new audit policies and also use the predefined audit policies. The audit records for these policies write to the unified audit trail. The earlier audit trails and their audit records remain, but no new audit records write to the earlier audit trails.

  > **Note:**
  >
  > The audit configuration from the earlier release has no effect in the unified audit system. Only unified audit policies generate audit records inside the unified audit trail.

- Use a mixed-mode audit facility.

  The mixed-mode audit facility enables both traditional and unified auditing facilities to run simultaneously and applies to both new and upgraded databases. The mixed-mode unified auditing facility becomes available if you enable at least one of the unified auditing predefined audit policies. Audit records for these policies write to the unified audit trail. The audit configuration in the earlier release of Oracle Database is

also available, and the audit records for this configuration write to the earlier audit trails. If you decide that you prefer using the pure unified audit facility, then you can switch to it by following the procedure in "Migrating to Unified Auditing for Oracle Database" (#CHDFBBAG).

> **Note:**
>
> If the database is not writable, then audit records write to new format operating system files in the `$ORACLE_BASE/audit/$ORACLE_SID` directory.

> **See Also:**
>
> - *Oracle Database Security Guide* (../DBSEG/audit_config.htm#DBSEG356)for information about the predefined audit policies
> - *Oracle Database Security Guide* (../DBSEG/audit_config.htm#DBSEG703)for information about the `ora_SecureConfig` audit policy

4.6.13.2 Migrating to Unified Auditing for Oracle Database

In a multitenant container database (CDB) environment, perform the following procedure in the `root`. The procedure will migrate both the `root` and any assoicated PDBs to unified auditing.

To migrate your database to enable unified auditing:

1. Log in to SQL*Plus as user `SYS` with the `SYSDBA` privilege.

   ```
   sqlplus sys as sysdba Enter password: password
   ```

   In a Pluggable Databases environment, this login connects you to the `root`.

2. Run the following query to check if your Oracle database has already been migrated to unified auditing:

   ```
   SQL> SELECT VALUE FROM V$OPTION WHERE PARAMETER = 'Unified Auditing';
   ```

   If the output is for the `VALUE` column is `TRUE`, then unified auditing is already enabled in your database. See "Managing Earlier Audit Records After You Migrate to Unified Auditing" (#CHDHHIBB) for what you should do next. If the output is `FALSE`, then complete the remaining steps in this procedure.

3. Stop the database. For single-instance environments, enter the following commands from SQL*Plus:

   ```
   SQL> SHUTDOWN IMMEDIATE SQL> EXIT
   ```

   For Windows systems, stop the Oracle service:

   ```
   net stop OracleService%ORACLE_SID%
   ```

   For Oracle RAC installations, shut down each database instance as follows:

   ```
   srvctl stop database -db db_name
   ```

4. Stop the listener. (Stopping the listener is not necessary for Oracle RAC and Grid Infrastructure listeners.)

```
lsnrctl stop listener_name
```

You can find the name of the listener by running the `lsnrctl status` command. The name is indicated by the `Alias` setting.

5. Go to the `$ORACLE_HOME/rdbms/lib` directory.
6. Enable the unified auditing executable as follows:
   - For UNIX, run the following command:
     ```
     make -f ins_rdbms.mk uniaud_on ioracle ORACLE_HOME=$ORACLE_HOME
     ```
   - For Windows, rename the `%ORACLE_HOME%/bin/orauniaud12.dll.dbl` file to `%ORACLE_HOME%/bin/orauniaud12.dll`.
7. Restart the listener.

   ```
   lsnrctl start listener_name
   ```
8. Restart the database. Log in to SQL*Plus and then enter the `STARTUP` command as follows:

   ```
   sqlplus sys as sysoper Enter password: password SQL> STARTUP
   ```

   For Windows systems, start the Oracle service again.

   ```
   net start OracleService%ORACLE_SID%
   ```

   For Oracle RAC installations, start each database instance as follows:

   ```
   srvctl start database -db db_name
   ```

4.6.13.3 Managing Earlier Audit Records After You Migrate to Unified Auditing

After you complete the procedure to migrate Oracle Database to use unified auditing, any audit records that your database had before remain in their earlier audit trails. You can archive these audit records and then purge their audit trails. With unified auditing in place, any new audit records write to the unified audit trail.

> **See Also:**
>
> - "Archiving the Audit Trail" in *Oracle Database Security Guide* (../DBSEG/audit_admin.htm#DBSEG732)
> - "Purging Audit Trail Records" in *Oracle Database Security Guide* (../DBSEG/audit_admin.htm#DBSEG90934)

4.6.13.4 Removing the Unified Auditing Functionality

If after you have enabled your databases to use unified auditing and you decide that you do not want unified auditing, you can remove the unified auditing functionality. In this case, your database uses the mixed-mode audit facility as described in "Migrating to Unified Auditing for Oracle Database" (#CHDFBBAG).

To remove unified auditing:

1. Stop the database.

```
sqlplus sys as sysoper Enter password: password SQL> SHUTDOWN IMMEDIATE SQL> EXIT
```

For Windows systems, stop the Oracle service:

```
net stop OracleService%ORACLE_SID%
```

For Oracle RAC installations, shut down each database instance as follows:

```
srvctl stop database -db db_name
```

2. Go to the `$ORACLE_HOME/rdbms/lib` directory.
3. Disable the unified auditing executable.
   - **UNIX:** Run the following command:
     ```
     make -f ins_rdbms.mk uniaud_off ioracle ORACLE_HOME=$ORACLE_HOME
     ```
   - **Windows:** Rename the `%ORACLE_HOME%/bin/orauniaud12.dll` file to `%ORACLE_HOME%/bin/orauniaud12.dll.dbl`.
4. Restart the database.

   ```
   sqlplus sys as sysoper Enter password: password SQL> STARTUP SQL> EXIT
   ```

   For Windows systems, start the Oracle service again.

   ```
   net start OracleService%ORACLE_SID%
   ```

   For Oracle RAC installations, start each database instance as follows:

   ```
   srvctl start database -db db_name
   ```

4.6.13.5 Documentation References if You Choose Not to Use Unified Auditing

After upgrading to Oracle Database 12*c*, if you choose not to change to unified auditing, then you can find information about traditional non-unified auditing from Oracle documentation and from Oracle Technology Network.

Refer to information about non-unified auditing at the following locations:

- *Oracle Database Security Guide*: This guide is the main source of information for configuring auditing. You must use the Oracle Database Release 11*g* version of this manual. To access this guide:
  1. Visit Oracle Technology Network at the following URL:

     `http://www.oracle.com/technetwork/index.html` (`http://www.oracle.com/technetwork/index.html`)

  2. From the Downloads menu, under **Databases**, select **Database 11g**.
  3. In the Downloads page, select the **Documentation** tab.
  4. From the most recent Oracle Database 11g Release 2 (11.2) Documentation page, select the **View Library** link to display the home page of the Release 11*g* documentation set.

5. Under the **Search** field, select the **Master Book List** link.

6. Search for **Security Guide**.

7. Select either the **HTML** or the **PDF** link for this guide.

- *Oracle Database SQL Language Reference* (../SQLRF/statements_4008.htm#SQLRF56110): This guide explains how to use the `AUDIT` (../SQLRF/statements_4007.htm#SQLRF01107)and `NOAUDIT` (../SQLRF/statements_9018.htm#SQLRF01607) statements for both unified auditing and non-unified auditing environments.

- *Oracle Database Reference* (../REFRN/GUID-82C7E258-EEF7-48D2-B06B-7F949686E54B.htm#REFRN10004) This guide explains how to use the initialization parameters and data dictionary views that are associated with a non-unified auditing environment. For a list of these, see *Oracle Database Security Guide* (../DBSEG/audit_changes.htm#DBSEG341).

- *Oracle Database Vault Administrator's Guide* (../DVADM/audplcy.htm#DVADM011) : This guide explains how to configure auditing in a non-unified auditing environment for Database Vault.

- *Oracle Label Security Administrator's Guide* (../OLSAG/audit.htm#OLSAG073): This guide explains how to configure auditing in a non-unified auditing environment for Oracle Label Security.

4.6.14 Test the Upgraded Production Oracle Database

If you upgraded a test database to the new Oracle Database release and then tested it, then you can now repeat those tests on the production database that you upgraded to the new Oracle Database 12*c* release. Compare the results, noting anomalies. Repeat the test upgrade as many times as necessary.

Test the newly upgraded production database with existing applications to verify that they operate properly with a new Oracle database. You also might test enhanced functions by adding available Oracle Database features. However, first ensure that the applications operate in the same manner as they did before the upgrade.

> **See Also:**
>
> Chapter 5, "Upgrading Applications After Upgrading Oracle Database" (app.htm#BABHJHEH) for more information on using applications with Oracle Database

4.7 Recommended Tasks After Upgrading an Oracle RAC Database

Oracle Real Application Clusters 12*c* Release 1 (12.1) uses the Single Client Access Name (SCAN). The SCAN is a single name that resolves to three IP addresses in the public network. When a release of an Oracle RAC database earlier than release 11.2 is upgraded, it is registered with SCAN listeners as remote listeners, and also continues to register with all node listeners. You can configure clients to use SCANs, or continue to use the node listeners. If you migrate all of your client connections to use SCANs, you can then remove the node listeners from the `REMOTE_LISTENERS` parameter. However, you cannot remove the listeners themselves, because only node listeners can create dedicated servers for the database.

> **See Also:**
>
> *Oracle Clusterware Administration and Deployment Guide* (../CWADD/intro.htm#CWADD92091) for more information on the Single Client Access Name (SCAN)

4.8 Recommended Tasks After Upgrading Oracle ASM

After you have upgraded Oracle ASM, Oracle recommends that you perform tasks such as resetting the Oracle ASM passwords and configuring disk groups.

The following tasks are recommended after upgrading Oracle ASM:

- Create A Shared Password File in the ASM Diskgroup (#CHDEJJAJ)
- Reset Oracle ASM Passwords to Enforce Case-Sensitivity (#CEGHIIIB)
- Advance the Oracle ASM and Oracle Database Disk Group Compatibility (#CEGJDCDD)
- Set Up Oracle ASM Preferred Read Failure Groups (#CEGICCFA)

You should also consider performing the following tasks, discussed earlier in this chapter:

- "Add New Features as Appropriate" (#CEGHDJEF)
- "Develop New Administrative Procedures as Needed" (#CEGFIHCI)

4.8.1 Create A Shared Password File in the ASM Diskgroup

If you advanced the `COMPATIBLE.ASM` disk group attribute to 12.1, then you must create a shared password file in the ASM diskgroup. See *Oracle Automatic Storage Management Administrator's Guide* (../OSTMG/GUID-DB3721CE-B1F4-4FB4-B290-B6D33BEAA5F2.htm#OSTMG95331)for complete information about managing a shared password file in a disk group.

4.8.2 Reset Oracle ASM Passwords to Enforce Case-Sensitivity

You can enforce case sensitivity for passwords. For example, the password `hPP5620qr` fails if it is entered as `hpp5620QR` or `hPp5620Qr`.

In releases earlier than Oracle Database 11*g* Release 1 (11.1), passwords were not case sensitive. To take advantage of enforced case-sensitive passwords, you must reset the passwords of existing users during the database upgrade procedure. For new Oracle Oracle ASM instances, there are no additional tasks or management requirements. For upgraded Oracle ASM instances, each user password must be reset with an `ALTER USER` statement.

> **Note:**
>
> If the default Oracle Database security settings are in place, then passwords must be at least eight characters, and passwords such as `welcome` and `oracle` are not allowed. See *Oracle Database Security Guide* (../DBSEG/guidelines.htm#DBSEG10005)for more information.

4.8.3 Advance the Oracle ASM and Oracle Database Disk Group Compatibility

You can advance the Oracle Database and the Oracle ASM disk group compatibility settings across software versions.

> **Caution:**

> If you advance the `COMPATIBLE.RDBMS` attribute, then you *cannot* revert to the previous setting. Therefore, before advancing the `COMPATIBLE.RDBMS` attribute, ensure that the values for the `COMPATIBLE` initialization parameter for all of the databases that use the disk group are set to at least the new setting for `COMPATIBLE.RDBMS` before you advance the attribute value.

Advancing compatibility enables new features only available in the new release. However, doing so makes the disk group incompatible with older releases of the software. Advancing the on disk compatibility is an irreversible operation.

You use the `compatible.rdbms` and `compatible.asm` attributes to specify the minimum software release required by the database instance and the Oracle ASM instance, respectively, to access the disk group. For example, the following `ALTER DISKGROUP` statement advances the Oracle ASM compatibility of the disk group `asmdg2`:

```
ALTER DISKGROUP asmdg2 SET ATTRIBUTE 'compatible.asm' = '11.2'
```

In this case, the disk group can be managed only by Oracle ASM software of release 11.2 or later, while any database client of release 10.2 or later can use the disk group.

> **See Also:**
>
> *Oracle Automatic Storage Management Administrator's Guide* (../OSTMG/GUID-AE540604-92D9-4CFE-A40E-BF4486163772.htm#OSTMG10045)for complete information about disk group compatibility, and *Oracle Database SQL Language Reference* (../SQLRF/statements_1009.htm#SQLRF01113)for more information about the disk group compatibility attributes on the `ALTER DISKGROUP` and `CREATE DISKGROUP` statements

4.8.4 Set Up Oracle ASM Preferred Read Failure Groups

Oracle ASM administrators can specify some disks to be preferred over others for read i/o operations. When Oracle ASM preferred read failure groups are defined, Oracle ASM can read from the extent that is closest to it, rather than always reading the primary copy.

> **See Also:**
>
> - *Oracle Clusterware Administration and Deployment Guide* (../CWADD/toc.htm) for information about specifying failure groups settings in an extended cluster
> - *Oracle Automatic Storage Management Administrator's Guide* (../OSTMG/toc.htm) for complete information about Oracle ASM preferred read failure groups, and specifying the new `ASM_PREFERRED_READ_FAILURE_GROUPS` initialization parameter to list failure group names that contain the preferred read disks for each node in a cluster
> - *Oracle Database Reference* (../REFRN/GUID-184C54A6-24CC-4A19-AA81-35AA76FF22A1.htm#REFRN10279)for the `ASM_PREFERRED_READ_FAILURE_GROUPS` initialization parameter

4.9 Recommended Tasks After Upgrading Oracle Database Express Edition

An Oracle Database Express database contains only a subset of the components available in an Oracle Database Standard Edition or Oracle Database Enterprise Edition database. After upgrading to the new Oracle Database release, you can use the Database Configuration Assistant (DBCA) to install additional components

into your database.

4.10 Optionally Update Oracle Application Express Packaged Applications

If your database originally included Oracle Application Express version 4.2 or up to version 4.2.5.00.08, then the 4.2.5 patch set was applied. However, the packaged applications that are shipped with Oracle Application Express were not updated to the 4.2.5 versions when the patch set was applied. You will need to run a script to update the packaged applications. If Oracle Application Express is installed in a non-CDB or is installed locally in a PDB, follow the instructions provided here.

To update the packaged applications in a non-CDB:

1. Set your current directory to the top-level "apex" directory in the Oracle home.
2. Start SQL*Plus and connect to the database where Oracle Application Express is installed as SYS specifying the SYSDBA role.

   On Windows:

   ```
   C:\ sqlplus /nolog SQL> CONNECT SYS as SYSDBA Enter password: SYS_password
   ```

   On Linux:

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

3. Run `apex_pkgapp_ins.sql` as shown in the following example:

   ```
   @apex_pkgapp_ins.sql
   ```

To update the packaged applications in a CDB:

1. Set your current directory to the top-level "apex" directory in the Oracle home.
2. Start SQL*Plus and connect to the database where Oracle Application Express is installed as SYS specifying the SYSDBA role.

   On Windows:

   ```
   C:\ sqlplus /nolog SQL> CONNECT SYS as SYSDBA Enter password: SYS_password
   ```

   On Linux:

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

3. Run `apex_pkgapp_con.sql` as shown in the following example:

   ```
   @apex_pkgapp_con.sql
   ```

4.11 Tasks to Complete Only After Manually Upgrading Oracle Database

If you are performing a manual upgrade of Oracle Database rather than using DBUA, then you must perform required tasks after your database is upgraded.

- Change Passwords for Oracle Supplied Accounts (#CEGBFEID)
- Create or Migrate Your Password File with ORAPWD (#CEGGIHGE)
- Migrate Your Initialization Parameter File to a Server Parameter File (#CEGGJJBD)
- Upgrade Oracle Text (#CEGJAFJJ)
- Upgrade the Oracle Clusterware Configuration (#CEGEJHEI)
- Adjust the Initialization Parameter File for the New Release (#CEGCIDAF)
- Set CLUSTER_DATABASE Initialization Parameter For Oracle RAC (#CEGCFJJC)

4.11.1 Change Passwords for Oracle Supplied Accounts

Depending on the release from which you upgraded, there might be new Oracle supplied accounts. Oracle recommends that you lock all Oracle supplied accounts except for `SYS` and `SYSTEM`, and expire their passwords, thus requiring new passwords to be specified when the accounts are unlocked.

> **Note:**
>
> If the default Oracle Database 12*c* security settings are in place, then passwords must be at least eight characters, and passwords such as `welcome` and `oracle` are not allowed. See *Oracle Database Security Guide* (../DBSEG/guidelines.htm#DBSEG10005)for more information.

You can view the status of all accounts by issuing the following SQL statement:

```
SQL> SELECT username, account_status FROM dba_users ORDER BY username;
```

To lock and expire passwords, issue the following SQL statement:

```
SQL> ALTER USER username PASSWORD EXPIRE ACCOUNT LOCK;
```

4.11.2 Create or Migrate Your Password File with ORAPWD

If the `REMOTE_LOGIN_PASSWORDFILE` initialization parameter is set to either `exclusive` or `shared`, create or migrate the password file with `ORAPWD`. Oracle Database 12*c* provides a new option to `ORAPWD` for migrating the password file from your existing database.

> **See Also:**
>
> *Oracle Database Administrator's Guide* (../ADMIN/dba.htm#ADMIN11059)for more information about creating or migrating password files

4.11.3 Migrate Your Initialization Parameter File to a Server Parameter File

If you are currently using a traditional initialization parameter file, then perform the following steps to migrate to a server parameter file:

1. If the initialization parameter file is located on a client computer, then transfer the file from the client computer to the server computer.

   > **Note:**
   >
   > If you are using Oracle RAC, then you must combine all of your instance-specific initialization parameter files into a single initialization parameter file. Instructions and other actions unique to using a server parameter file for cluster databases, are discussed in:
   >
   > - *Oracle Real Application Clusters Administration and Deployment Guide* (../RACAD/toc.htm)
   > - The *Oracle Real Application Clusters Installation Guide* (http://www.oracle.com/pls/topic/lookup?ctx=E50529-01&id=RIGEN)for your operating system

2. Create a server parameter file using the `CREATE SPFILE` statement. This statement reads the initialization parameter file to create a server parameter file. You are not required to start the database to issue a `CREATE SPFILE` statement.

3. Start up the instance using the newly-created server parameter file.

> **See Also:**
>
> - *Oracle Database Administrator's Guide* (../ADMIN/create.htm#ADMIN00202)for more information about creating server parameter files
> - *Oracle Database SQL Language Reference* (../SQLRF/statements_6018.htm#SQLRF01315)for information about the `CREATE SPFILE` statement

4.11.4 Upgrade Oracle Text

After an upgrade to the new Oracle Database 12*c* release, copy the following files from the previous Oracle home to the new Oracle home:

- Stemming user-dictionary files
- User-modified `KOREAN_MORPH_LEXER` dictionary files
- `USER_FILTER` executables

These files affect all databases installed in the given Oracle home.

You can obtain a list of these files as follows:

1. Read the text file at `$ORACLE_HOME/ctx/admin/ctxf102.txt`.
2. Run `$ORACLE_HOME/ctx/admin/ctxf102.sql` as database user `SYS`, `SYSTEM`, or `CTXSYS`.

> **See Also:**
>
> - *Oracle Text Reference* (../CCREF/cdatadic.htm#CCREF1901)for more information about these files

- *Oracle Text Application Developer's Guide* (../CCAPP/GUID-2D2548BE-879D-4B44-BF01-AC62CACA4782.htm#CCAPP2001)for information about upgrading your applications from previous releases of Oracle Text

4.11.5 Upgrade the Oracle Clusterware Configuration

If you are using Oracle Clusterware, then you must upgrade the Oracle Clusterware keys for the database.

Run `srvctl` for Oracle Database 12*c* to upgrade the database. For example:

```
ORACLE_HOME/bin/srvctl upgrade database -db name -o ORACLE_HOME
```

See Also:

Oracle Real Application Clusters Administration and Deployment Guide (http://www.oracle.com/pls/topic/lookup?ctx=E50529-01&id=RACAD8296)for the syntax for `srvctl upgrade database`

4.11.6 Adjust the Initialization Parameter File for the New Release

Each release of Oracle Database introduces new initialization parameters, deprecates some initialization parameters, and desupports some initialization parameters. You must adjust the parameter file to account for these changes and to take advantage of new initialization parameters that might be beneficial to your system. Additionally, when you perform a manual upgrade without using DBUA, the `tnsnames.ora` file is not automatically populated with new configuration information and settings. Therefore, you must manually update `tnsnames.ora` and adjust `local_listener` and `remote_listener` parameter references if these must be resolved.

See Also:

- The "What's New in Oracle Database Reference" section of *Oracle Database Reference* (../REFRN/toc.htm) for a list of the new initialization parameters in Oracle Database 12*c*, and for information about each parameter
- Chapter 8, "Deprecated and Desupported Features for Oracle Database 12*c*" (deprecated.htm#BABBIBFB)for desupported and deprecated initialization parameters in Oracle Database 12*c*
- Appendix A, "Changes for Earlier Releases of Oracle Database" (changes.htm#BABHACIE)

4.11.6.1 Setting the COMPATIBLE Initialization Parameter

The `COMPATIBLE` initialization parameter controls the compatibility level of your database. When you are certain that you no longer need the ability to downgrade your database to its original release, set the `COMPATIBLE` initialization parameter based on the compatibility level you want for your new database.

Complete the following steps to set the `COMPATIBLE` initialization parameter to a higher value:

1. Perform a backup of your database before you raise the `COMPATIBLE` initialization parameter (optional).

Raising the COMPATIBLE initialization parameter might cause your database to become incompatible with earlier releases of Oracle Database, and a backup ensures that you can return to the earlier release if necessary.

> **See Also:**
>
> *Oracle Database Backup and Recovery User's Guide* (../BRADV/toc.htm) for more information about performing a backup

2. If you are using a server parameter file, then complete the following steps:

   a. Update the server parameter file to set or change the value of the COMPATIBLE initialization parameter.

      For example, to set the COMPATIBLE initialization parameter to 11.0.0, enter the following statement:

      ```
      SQL> ALTER SYSTEM SET COMPATIBLE = '11.0.0' SCOPE=SPFILE;
      ```

   b. Shut down and restart the instance.

> **Note:**
>
> When upgrading systems with HARD-compliant storage (Hardware Assisted Resilient Data), consider the following:
>
> - If the COMPATIBLE parameter is set to a release number earlier than 11.0.0, then you cannot locate the server parameter file (SPFILE) on HARD storage.
> - If the COMPATIBLE parameter is set to 11.0.0, then you can optionally locate the server parameter file on HARD storage.
>
> Because the default SPFILE location (*ORACLE_HOME*/dbs) might not be on a HARD-compliant storage system, it is likely you must provide a parameter file that specifies the location of the SPFILE.

3. If you are using an initialization parameter file, then complete the following steps:

   a. Shut down the instance if it is running:

      ```
      SQL> SHUTDOWN IMMEDIATE
      ```

   b. Edit the initialization parameter file to set or change the value of the COMPATIBLE initialization parameter.

      For example, to set the COMPATIBLE initialization parameter to `for Oracle Database release 12.1`, enter the following in the initialization parameter file:

      ```
      COMPATIBLE = 12.1.0
      ```

   c. Start the instance using STARTUP.

> **Note:**
>
> If you are using an ASM disk group, then the disk group's compatibility attribute must match or be lower than that of the database compatibility parameter in `init.ora`.

4.11.6.2 Configuring tnsnames.ora and Listener Parameters

After performing a manual upgrade, you must adjust `local_listener` and `remote_listener` parameter references if they must be resolved in `tnsnames.ora`. DBUA handles changes to network naming and listeners during automatic upgrades, but during a manual upgrade, `tnsnames.ora` is not changed, nor are the listeners.

> **See Also:**
>
> - Local Naming Parameters (tnsnames.ora) in *Oracle Database Net Services Reference* (../NETRF/tnsnames.htm#NETRF007)
> - "Configuring the tnsnames.ora File After Installation" in *Oracle Database Net Services Administrator's Guide* (../NETAG/naming.htm#NETAG259)
> - "Configuring and Administering Oracle Net Listener" in *Oracle Database Net Services Administrator's Guide* for information on registering information with a local listener and a remote listener (../NETAG/listenercfg.htm#NETAG010)
> - "Net Service Names (tnsnames.ora File)" in *Oracle Real Application Clusters Installation Guide for Microsoft Windows x64 (64-Bit)* (../RIWIN/toc.htm) for Windows
> - "Net Service Names (tnsnames.ora File)" in *Oracle Real Application Clusters Installation Guide for Linux and UNIX* (../RILIN/undrstnd.htm#RILIN610)

4.11.7 Set CLUSTER_DATABASE Initialization Parameter For Oracle RAC

For upgrades of Oracle RAC databases, in "Preparing the New Oracle Home for Upgrading" (preup.htm#BABGBFCJ) you were instructed to set the `CLUSTER_DATABASE` initialization parameter to `false` before upgrading a cluster database. Now that the upgrade is finished, you must set this parameter to `true`.

(#)
About Oracle (http://www.oracle.com/corporate/index.html) | Contact Us (http://www.oracle.com/us/corporate/contact/index.html) | Legal Notices (http://www.oracle.com/us/legal/index.html) | Terms of Use (http://www.oracle.com/us/legal/terms/index.html) | Your Privacy Rights (http://www.oracle.com/us/legal/privacy/index.html)
Copyright © 2002, 2015, Oracle and/or its affiliates. All rights reserved. (http://www.oracle.com/pls/topic/lookup?ctx=cpyr&id=en)