26

Performing Post-Upgrade Tasks

ORACLE

Objectives

After completing this lesson, you should be able to:

- Perform post-upgrade tasks
- Migrate to Unified Auditing

Required Tasks After Database Upgrade

Perform the following tasks as appropriate to your environment:

- For a manual upgrade:
  - Update the `ORACLE_HOME` and `PATH` operating system environment variables
  - Update the `oratab` file with the new Oracle home
- For all upgrade methods, update client scripts with the new Oracle home
- Upgrade the RMAN Recovery Catalog
- Configure the FTP and HTTP ports, and HTTP authentication for Oracle XML DB
- Enable Database Vault

After you upgrade to Oracle Database 12*c* and before you can consider the database operational, you must complete some postupgrade tasks. The tasks you need to complete depend on whether you performed a manual upgrade or used DBUA, and also on your configuration and use of features. Some common tasks include the following:

- Updating the environment variables following a manual upgrade: On Linux and UNIX operating systems, ensure that the `ORACLE_HOME` and `PATH` environment variables point to the new Oracle home.
- Updating the `oratab` file and client scripts with the new Oracle home: DBUA automatically points `oratab` to the new Oracle home. Regardless of the upgrade method you must check client scripts.
- Upgrading the RMAN Recovery Catalog: If the recovery catalog schema version is older than what is required by the RMAN client, you must upgrade it.
- Configuring the FTP and HTTP ports, and HTTP authentication for Oracle XML DB: The Oracle Database 12*c* DBCA does not configure ports for Oracle XML DB so you must manually configure them. You should also configure digest authentication for HTTP to take advantage of improved security features.
- Enabling Database Vault: Register Database Vault by using the `DVSYS.DBMS_MACADM.ENABLE_DV` procedure.

Recommended Tasks After Database Upgrade

It is recommended that you perform the following tasks after upgrading to Oracle Database 12*c*:

- Reset passwords to enforce case-sensitivity.
- Set threshold values for tablespace alerts.
- Implement new features as appropriate.
- Migrate to unified auditing.

You should consider the recommended tasks that are listed in the slide depending on the release you have migrated from and your use of various features. Additional information about each task follows and more detail can be found in the *Oracle Database Upgrade Guide 12c Release 1 (12.1)*:

- Reset passwords to enforce case-sensitivity: 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. You can execute the `DBMS_VERIFIER.EXPIRE_ACCOUNTS_WITHOUT_LATEST_VERIFIER` procedure that forces users whose accounts do not yet have the latest verifier to change their passwords the next time they log in.
- Set threshold values for tablespace alerts: In an upgraded Oracle Database 12*c* database, Tablespace Alerts are disabled (the thresholds are set to null). Tablespaces in the database that are candidates for monitoring must be identified and the appropriate threshold values must be set. The default threshold values for a newly created Oracle Database 12*c* database are:
  - 85% full warning
  - 97% full critical

- Implement new features: Refer to the *Oracle Database New Features Guide* for a description of the new features in Oracle Database 12*c*. Attend the Oracle Database 12*c*: New Features for Administrators course to learn more about the new features.
- Migrate to unified auditing: Oracle Database 12*c* includes a new feature called the unified audit trail. With unified auditing, all Oracle Database audit trails (`SYS.AUD$` for the database audit trail, `SYS.FGA_LOG$` for fine-grained auditing, `DVSYS.AUDIT_TRAIL$` for Database Vault, and so on) are consolidated into one single audit trail. Additional information about unified auditing follows in this lesson.

Understanding Auditing Implementation

- *Mixed mode auditing* is the default when a new Oracle Database 12*c* database is created.
- Mixed mode auditing enables the use of:
  - Pre–Oracle Database 12*c* auditing features
  - *Unified auditing* features of Oracle Database 12*c*
- The recommendation from Oracle is to migrate to unified auditing.
- Query `V$OPTION` to determine if the database has been migrated to unified auditing:

```
SELECT value FROM v$option
WHERE parameter = 'Unified Auditing'
```


Prior to Oracle Database 12*c*, audit records from various sources were stored in different locations. Oracle Database 12*c* supports *unified auditing*, in which all audit records are stored in a single audit table.

When you create a new Oracle Database 12*c* database, mixed mode auditing is enabled. This mode enables you to use the auditing features available before Oracle Database 12*c* and also the unified auditing features. Mixed mode auditing is enabled by default through the `ORA_SECURECONFIG` predefined auditing policy for newly created databases.

If you are upgrading a database to Oracle Database 12*c*, you must manually migrate to unified auditing to use the unified auditing features.

Oracle Corporation recommends that you migrate to unified auditing.

Enabling Unified Auditing

1. In SQL*Plus, shut down the database instance:

```
SQL> SHUTDOWN IMMEDIATE
```

2. Shut downr the listener:

```
$ lsnrctl stop
```

3. At the operating system prompt, enable the unified auditing executable:

```
$ cd $ORACLE_HOME/rdbms/lib
$ make -f ins_rdbms.mk uniaud_on ioracle ORACLE_HOME=$ORACLE_HOME
```

4. Restart the listener:

```
$ lsnrctl start
```

5. In SQL*Plus, restart the database instance:

```
SQL> STARTUP
```


Before enabling the unified auditing executable, shut down the database instance and the listener.

Change to the `$ORACLE_HOME/rdbms/lib` directory and execute the following command:

`make -f ins_rdbms.mk uniaud_on ioracle ORACLE_HOME=$ORACLE_HOME`

The `make` command is used to relink the Oracle executable with a different set of libraries to enable unified auditing.

After the `make` command completes, restart the listener and the database instance.

You can log in to SQL*Plus and verify that unified auditing has been enabled as follows:

```
SQL> select value
  2  from v$option
  3  where parameter = 'Unified Auditing';

VALUE
----------------------------------------------------------------
TRUE
```

Administering the Roles Required for Auditing

A user must be granted one of the following roles to perform auditing tasks:

- `AUDIT_ADMIN` enables the user to:
  - Create unified and fine-grained audit policies
  - Execute the `AUDIT` and `NOAUDIT` SQL statements
  - View audit data
  - Manage the audit trail (table in the `AUDSYS` schema)
- `AUDIT_VIEWER` enables the user to:
  - View and analyze audit data

Users must be granted the appropriate privilege to configure auditing and view audit data. To support separation of duty, two default roles are provided:

- `AUDIT_ADMIN`: Enables the grantee to configure auditing settings, create and administer audit policies (unified and fine-grained), and view and analyze audit data. This role is typically granted to a security administrator.
- `AUDIT_VIEWER`: Enables the grantee to view and analyze audit data. This role is typically granted to external auditors.

Summary

In this lesson, you should have learned how to:

- Perform post-upgrade tasks
- Migrate to Unified Auditing

Practice 26

26-1: Performing Post-Upgrade Actions