



## Oracle Data Guard

Oracle Data Guard is the most effective and comprehensive data availability, data protection and disaster recovery solution for enterprise databases.

Oracle Data Guard is the management, monitoring, and automation software infrastructure that creates, maintains, and monitors one or more standby databases to protect enterprise data from failures, disasters, errors, and corruptions.

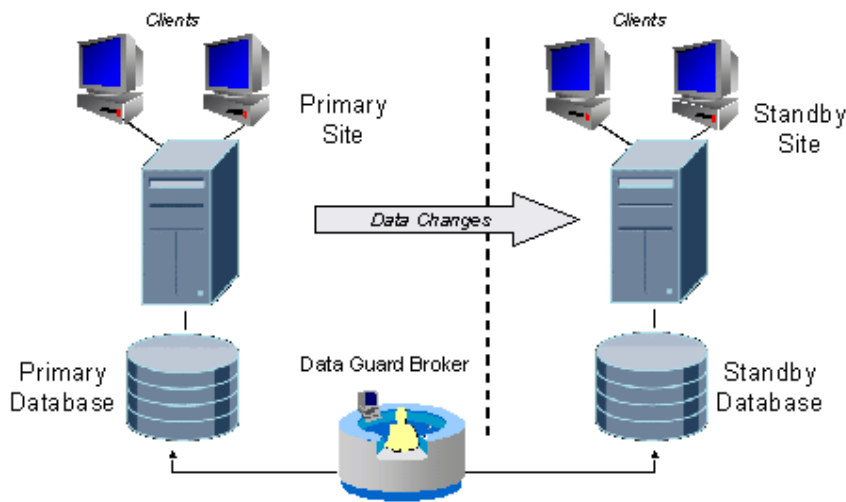
Data Guard maintains these standby databases as synchronized copies of the production database. These standby databases can be located at remote disaster recovery sites thousands of miles away from the production data center, or they may be located in the same city, same campus, or even in the same building. If the production database becomes unavailable because of a planned or an unplanned outage, Data Guard can switch any standby database to the production role, thus minimizing the downtime associated with the outage, and preventing any data loss.

Data Guard 11g builds upon an already unique set of capabilities, and redefines what users can expect from a disaster recovery solution. It can address both High Availability and Disaster Recovery requirements, and is the ideal complement to Oracle Real Application Clusters (Oracle RAC). Data Guard has the requisite knowledge of the Oracle database to reliably protect a standby database from corruptions that attempt to propagate from a primary database. It enables all standby databases, both physical and logical, to be used for productive purposes while in standby role. Data Guard delivers:

- Reliability— optimum data protection and availability. You always know the state of your standby database and it can very quickly (in seconds), assume the primary role.
- Lower cost and complexity – Data Guard's mature capabilities and rich management interface are included features of Oracle Enterprise Edition.
- Maximum return on investment – All standby databases can be utilized for production purposes while in standby role. Idle resources are eliminated.

Data Guard can be used in combination with other [Oracle High Availability \(HA\) solutions](#) such as [Real Application Clusters \(RAC\)](#), [Oracle Flashback](#), [Oracle Recovery Manager \(RMAN\)](#), and new database options for Oracle Database 11g that include [Oracle Active Data Guard](#) and [Oracle Advanced Compression](#), to provide a high level of data protection, data availability, and resource utilization that is unprecedented in the industry.

The following diagram presents a hi-level overview of Oracle Data Guard.



## Data Guard Benefits

### 1. *Disaster recovery and high availability*

Data Guard provides an efficient and comprehensive disaster recovery and high availability solution. Automatic failover and easy-to-manage switchover capabilities allow quick role reversals between primary and standby databases, minimizing the downtime of the primary database for planned and unplanned outages.

### 2. *Complete data protection*

A standby database also provides an effective safeguard against data corruptions and user errors. Storage level physical corruptions on the primary database do not propagate to the standby database. Similarly, logical corruptions or user errors that cause the primary database to be permanently damaged can be resolved. Finally, the redo data is validated at the time it is received at the standby database and further when applied to the standby database.

### 3. *Efficient utilization of system resources*

A physical standby database can be used for backups and read-only reporting, thereby reducing the primary database workload and saving valuable CPU and I/O cycles. A physical standby database can also be easily converted back and forth between being a physical standby database and an open read/write database, without compromising data protection. A logical standby database enables read-write access to a synchronized standby database, and/or adding local tables to the standby database that can also be updated, and/or creating additional indexes to optimize read performance.

### 4. *Flexibility in data protection to balance availability against performance requirements*

Oracle Data Guard offers the maximum protection, maximum availability, and maximum performance modes to help enterprises balance data availability against

system performance requirements.

#### 5. Protection from communication failures

If network connectivity is lost between the primary and one or more standby databases, redo data cannot be sent from the primary to those standby databases. Once connectivity is re-established, the missing redo data is automatically detected by Data Guard and the necessary archive logs are automatically transmitted to the standby databases. The standby databases are resynchronized with the primary database, with no manual intervention by the administrator.

#### 6. Centralized and simple management

Data Guard Broker automates the management and monitoring tasks across the multiple databases in a Data Guard configuration. Administrators may use either Oracle Enterprise Manager or the Broker's own specialized command-line interface (DGMGRL) to take advantage of this integrated management framework.

#### 7. Integrated with Oracle database

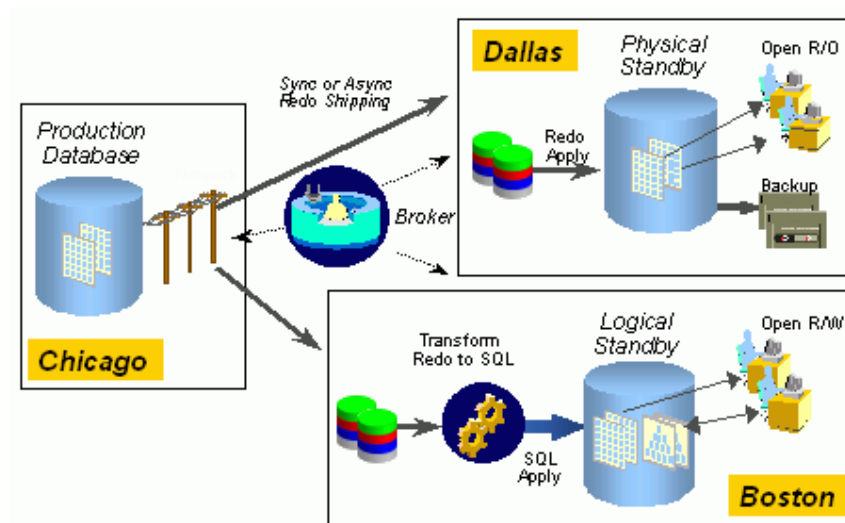
Data Guard is available as an integrated feature of the Oracle Database (Enterprise Edition) at no extra cost.

### Overview of Oracle Data Guard Functional Components

#### Data Guard Configuration

A Data Guard configuration consists of one production (or primary) database and up to nine standby databases. The databases in a Data Guard configuration are connected by Oracle Net and may be dispersed geographically. There are no restrictions on where the databases are located, provided that they can communicate with each other.

#### Data Guard Architecture Diagram



## Redo Apply and SQL Apply

A standby database is initially created from a backup copy of the primary database. Once created, Data Guard automatically maintains the standby database as a synchronized copy of the primary database by transmitting primary database redo data to the standby system and then applying the redo data to the standby database.

Data Guard provides two methods to apply this redo data to the standby database and keep it synchronized with the primary, and these methods correspond to the two types of standby databases supported by Data Guard.

- Redo Apply, used for physical standby databases
- SQL Apply, used for logical standby databases

A physical standby database provides a physically identical copy of the primary database, with on-disk database structures that are identical to the primary database on a block-for-block basis. The database schema, including indexes, are the same. The Redo Apply technology applies redo data on the physical standby database using standard Oracle media recovery techniques. In addition to traditional Data Guard functionality, the Active Data Guard Option for Oracle Database 11g enables a physical standby database to be open read-only while it applies updates received from the primary database. This makes physical standby databases useful for offloading the primary database from the overhead of processing read-only queries and reports. This also makes it simple to validate that the standby database is synchronized with the primary database at all times.

A logical standby database contains the same logical information as the production database, although the physical organization and structure of the data can be different. The SQL apply technology keeps the logical standby database synchronized with the primary database by transforming redo data received from the primary database into SQL statements and then executing the SQL statements on the standby database. This makes it possible for the logical standby database to be open read-write and accessed for queries and reporting purposes at the same time the SQL is being applied to it.

## Role Management

Using Data Guard, the role of a database can be switched from a primary role to a standby role and vice versa, ensuring no data loss in the process, and minimizing downtime. There are two kinds of role transitions - a switchover and a failover. A switchover is a role reversal between the primary database and one of its standby databases. This is typically done for planned maintenance of the primary system. During a switchover, the primary database transitions to a standby role and the standby database transitions to the primary role. The transition occurs without having to re-create either database. A failover is a transition of a standby database to the primary role following a sudden outage of the primary database. The failed primary can be reinstated as a standby database for the new primary using Oracle Flashback Database. This can eliminate the need to recreate the failed primary from a backup, dramatically reducing the time and effort required to return the configuration to a protected state. Administrators have the option of executing failovers manually, or Data Guard can be configured to automatically detect primary database failures and execute a failover to the standby database without manual intervention.

## Data Guard Protection Modes

In some situations, a business cannot afford to lose data at any cost. In other situations,

some applications require maximum database performance and can tolerate a potential loss of data. Data Guard provides three distinct modes of data protection to satisfy these varied requirements:

- **Maximum Protection**—This mode offers the highest level of data protection. Data is synchronously transmitted to the standby database from the primary database and transactions are not committed on the primary database unless the redo data is available on at least one standby database configured in this mode. If the last standby database configured in this mode becomes unavailable, processing stops on the primary database. This mode ensures no-data-loss, even in the event of multiple failures.
- **Maximum Availability**—This mode is similar to the maximum protection mode, including zero data loss. However, if a standby database becomes unavailable (for example, because of network connectivity problems), processing continues on the primary database. When the fault is corrected, the standby database is automatically resynchronized with the primary database. This mode achieves no-data-loss in the event of a single failure (e.g. network failure, primary site failure . . .)
- **Maximum Performance**—This mode offers slightly less data protection on the primary database, but higher performance than maximum availability mode. In this mode, as the primary database processes transactions, redo data is asynchronously shipped to the standby database. The commit operation of the primary database does not wait for the standby database to acknowledge receipt of redo data before completing write operations on the primary database. If any standby destination becomes unavailable, processing continues on the primary database and there is little effect on primary database performance.

### Data Guard Broker

The Oracle Data Guard Broker is a distributed management framework that automates and centralizes the creation, maintenance, and monitoring of Data Guard configurations. All management operations can be performed either through Oracle Enterprise Manager, which uses the Broker, or through the Broker's specialized command-line interface (DGMGRL). Data Guard Broker 11g also enables automatic database failover for Data Guard configurations using either Maximum Availability or Maximum Performance modes.

### What's New in Oracle Data Guard 11g?

Data Guard 11g has been made even more straightforward to implement and manage using either the Data Guard broker command line interface or Enterprise Manager Grid Control. Data Guard 11g adds new ways to detect corruptions that avoid data loss and extended down time. Data Guard 11g includes flexible configuration options for fast, automatic failover in both Maximum Availability and Maximum Performance protection modes. Data Guard 11g physical standby databases can offload the primary database of queries and reporting by being open read-only while apply is active, effectively creating a new level of performance protection and return on investment for every Data Guard environment. The sections below highlight some of the key new features of Oracle Data Guard 11g. For details, please refer to the following:

- [Technical white paper on Oracle Data Guard 11g](#)

## Snapshot Standby

This is a new type of standby database that is created from a physical standby database. Once created, a snapshot standby can be opened read-write to process transactions that are independent of the primary database for test or other purposes. A snapshot standby will continue to receive and archive updates from the primary database, however, redo data received from the primary will not be applied until the snapshot standby is converted back into a physical standby database and all updates that were made to it while it was a snapshot standby are discarded. The ability for the snapshot standby to archive data received from the primary while the snapshot is open read-write means production data stays protected at all times.

## Support for the Oracle Active Data Guard Option

The [Active Data Guard Option](#) enhances Quality of Service by offloading resource intensive workloads from your production database to one or more synchronized standby databases. Active Data Guard accomplishes this by enabling read-only access to a physical standby database for queries, real-time reporting, web-based access, etc., while continuously applying changes received from the production database. Active Data Guard also eliminates the overhead of performing backups on production systems by enabling RMAN block-change tracking and fast incremental backups using a physical standby database.

## Failover enhancements

Data Guard 10g Release 2 introduced automatic failover using the new feature Fast-Start Failover with Maximum Availability protection mode (SYNC). Data Guard 11g extends Fast-Start Failover support Maximum Performance mode (ASYNC) by adding a user configurable data loss threshold that guarantees an automatic failover will never result in data loss that exceeds the desired recovery point objective (RPO).

Users can also configure an automatic failover to occur immediately without waiting for the Fast-Start Failover threshold time period to expire based on designated health check conditions or any desired ORA-nnnnn error.

A new DBMS\_DG PL/SQL package can be used to enable applications to notify the Fast-Start Failover Observer process to initiate an automatic failover.

Other enhancements enable faster failovers across a range of Data Guard configurations – both manual and automatic failovers, and both logical and physical standby databases.

## Enhanced data protection

A Physical Standby can detect lost datafile writes caused by faulty storage hardware and firmware that lead to data corruption on either the primary or the standby database. Data Guard will compare versions of blocks on the standby with that of the incoming redo stream. If there is a version discrepancy it implies a lost write. The user can then failover to the standby database and restore data consistency..

## Redo Transport enhancements

Data Guard 11g implements a new streaming design that significantly increases the throughput of redo transport in Maximum Performance protection mode (during asynchronous redo transport and when using ARCn processes to resolve gaps). The benefit of these enhancements will be particularly noticeable in high latency – WAN environments.

Enhancements to synchronous redo transport in Maximum Availability mode will further reduce the impact of network latency on primary database throughput, expanding the number of applications that will be able to tolerate synchronous zero data loss protection, and extending the distance between primary and standby databases that is practical for such implementations.

Faster resynchronization of standby databases following network or standby database outages when using the Oracle Advanced Compression Option. One of the capabilities of the Advanced Compression Option enables automatic network compression of archive logs shipped by Data Guard to resolve gaps on the standby database. This feature is particularly beneficial for bandwidth constrained, high latency network environments.

#### Apply performance enhancements

Parallel media recovery significantly enhances Redo Apply performance (physical standby) for all workload profiles.

SQL Apply enhancements for logical standby increase apply performance for inserts and updates to tables that are not partitioned and that do not contain LOB, LONG or XML type column. Also, SQL Apply now applies parallel DDL in parallel, rather than serially as was the practice in previous releases.

#### Transient Logical Standby

Users can convert a physical standby to a transient logical standby database to effect a rolling database upgrade, and then revert the standby to its original state as a physical standby database once the upgrade is complete - using the `KEEP IDENTITY` clause. This benefits physical standby users who wish to execute a rolling database upgrade without investing in redundant storage otherwise needed to create a logical standby database.

#### Fine-grained monitoring of Data Guard configurations

Oracle Enterprise Manager has been enhanced to provide granular, up-to-date monitoring of Data Guard configurations, so that administrators may make an informed and expedient decision regarding managing this configuration.

#### RMAN enhancements for Data Guard

RMAN `DUPLICATE` can create standby databases directly from the primary database to the standby system without requiring interim storage at either location.

In addition to Real-time Query discussed above, the Active Data Guard Option adds support for RMAN block-change tracking on a physical standby database enabling fast incremental backup of a standby database. Tests have shown that incremental backups on a database with a moderate rate of change can complete up to 20x faster when using RMAN block-change tracking, compared to traditional incremental backups.

#### Enhanced security

SSL authentication can be used in lieu of password file to authenticate redo transmission. Note: SSL authentication requires use of PKI Certificates, the Oracle Advanced Security Option and Oracle Internet Directory.

## Enhanced SQL Apply support

- XMLType data type (when stored as CLOB)
- Ability to execute DDL in parallel on a logical standby database
- Transparent Data Encryption (TDE)
- DBMS\_FGA (Fine Grained Auditing)
- DBMS\_RLS (Virtual Private Database)

## SQL Apply Manageability

Scheduler jobs can be created on a standby database using the DBMS\_SCHEDULER package and can be associated with an appropriate database role such that they run when intended (e.g. when the database is the primary, standby, or both).

Switchover using SQL Apply with Oracle RAC databases no longer requires the prior shutdown of all but the first instance in each Oracle RAC cluster.

Data Guard SQL Apply parameters may also be set dynamically without requiring SQL Apply to be restarted. Using the DBMS\_LOGSTDBY.APPLY\_SET package, you can dynamically set initialization parameters, thus improving the manageability, uptime, and automation of a logical standby configuration.

## Data Guard Broker

- Enables automatic database failover for configurations using either Maximum Availability or Maximum Performance mode.
- Enables configurable events to trigger immediate automatic failover to a target standby database.
- Improved support for redo transport options, enabling an administrator to specify a connect description for Redo Transport Services.
- Elimination of database downtime when changing the protection mode to and from Maximum Availability and Maximum Performance.
- Support for single instance databases configured for HA using Oracle Clusterware and cold failover clusters.

## Enterprise Manager Grid Control 11g

- Creation of standby databases from existing RMAN backups
- Creation of an Oracle RAC standby database from an Oracle RAC primary
- Automated standby clones for reporting, development, and test
- Automatic propagation of Enterprise Manager jobs and metric thresholds to the new primary database upon switchover or failover
- Fault-tolerant observer for Fast-Start Failover
- Enterprise Manager Data Recovery Advisor will utilize available standby databases when making recommendations for Intelligent Data Repair (IDR)