Oracle archive log and data guard concept

1.What is Archive Log?

"archivelog mode" implies that the database itself will keep track of every change made by writting an entry in the Redolog Groups (there's at least 2 of them and the writes to the redolog will use them in a cycle changing from one to the next as they are getting full). Here it comes the difference between having the database in archivelog mode or not, if archivelog mode is active, the redolog contents will be saved onto files known as "archived logs". If the database is in noarchivelog mode, the redolog contents will be discarded.

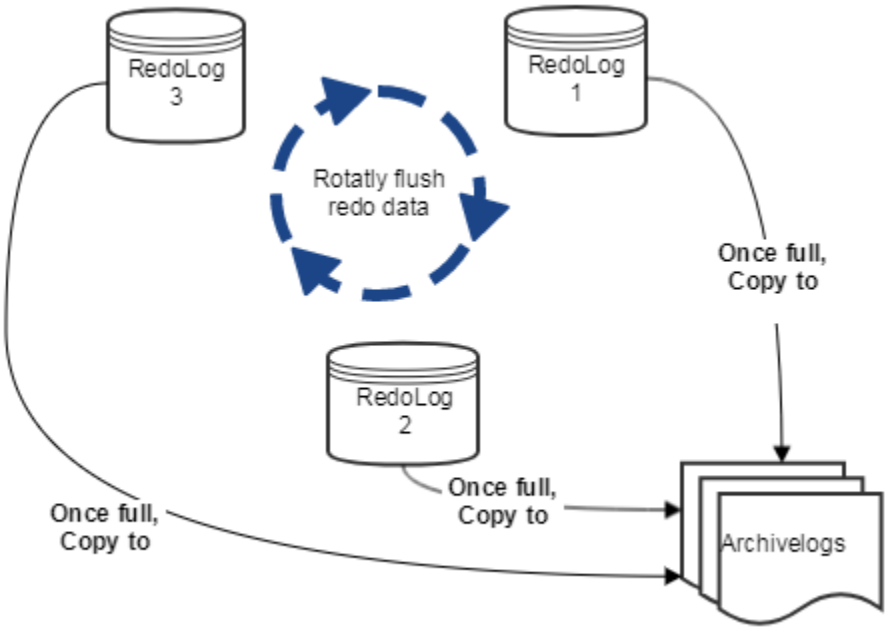
Archive log is full copies of oracle redo logs, redo log contains redo data in block level generated by database storage engine.

With Archive logs, DBA can recover and do hot backup(snapshot) from your production without stoping DB service.

1.1 What is redo log?

Oracle redo log is generated by database storage engine, with raw meta data used by storage engine to reproduce the transaction or roll back it.

1.2 How it works



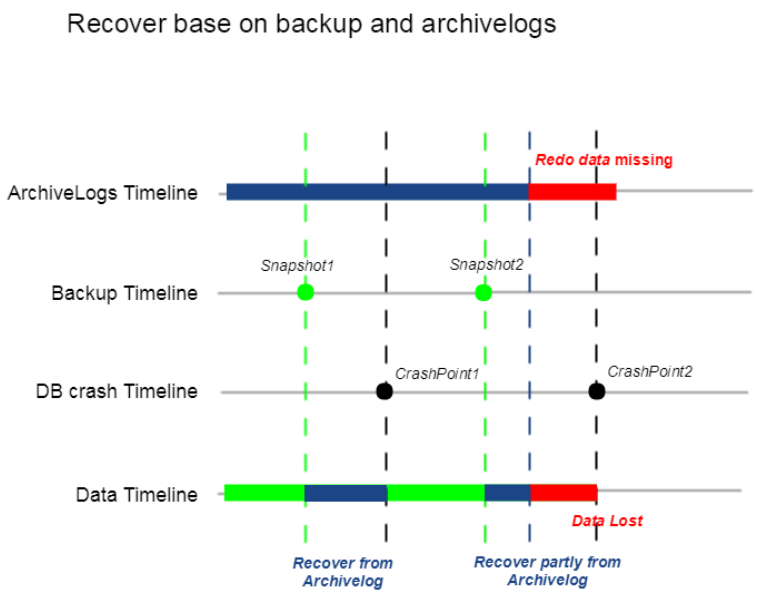
DBA usually config 3 redo log groups in achivelog mode, otherwise there are 2 redo logs groups in default.

Oracle storage engine generate the redo data and save it into redo log between the redo log groups rotally once the log file is full.

1.3 Comparing the Archive/NoArchive log mode

	Archivelog mode	Noarchivelog mode
Cold Backup	Yes	Yes, limited. Shut DB down.
Hot Backup	Yes	No

1.4 Recover from backup and archivelog.



In production, DBA usually do the backup of database intervally, for example the 2 snapshot points in the backup timeline here. If the crashPoint1 happens, then DBA can

recover the data from snapshot1 plus the redo data in arcivelog between time snapshot1 to crashpoint1.

Without full context of archive log, data lost might be happens. for example the recover of crashpoint2, DBA can only recover the data from snapshot2 plus only available archivelog, those redo data not saved in redo log can not recovered.

2. Data guard concept

Oracle Data Guard ensures high availability, data protection, and disaster recovery for enterprise data.

2.1 Data Guard Configurations

An Oracle Data Guard configuration can contain one primary database and up to thirty destinations.

2.1.1 Primary Database

An Oracle Data Guard configuration contains one production database, also referred to as the primary database, that functions in the primary role.

2.1.2 Standby Databases

A standby database is a transactionally consistent copy of the primary database.

The types of standby databases are as follows:

- **Physical standby database (Redo data apply)**

  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.

- **Logical standby database (SQL apply)**

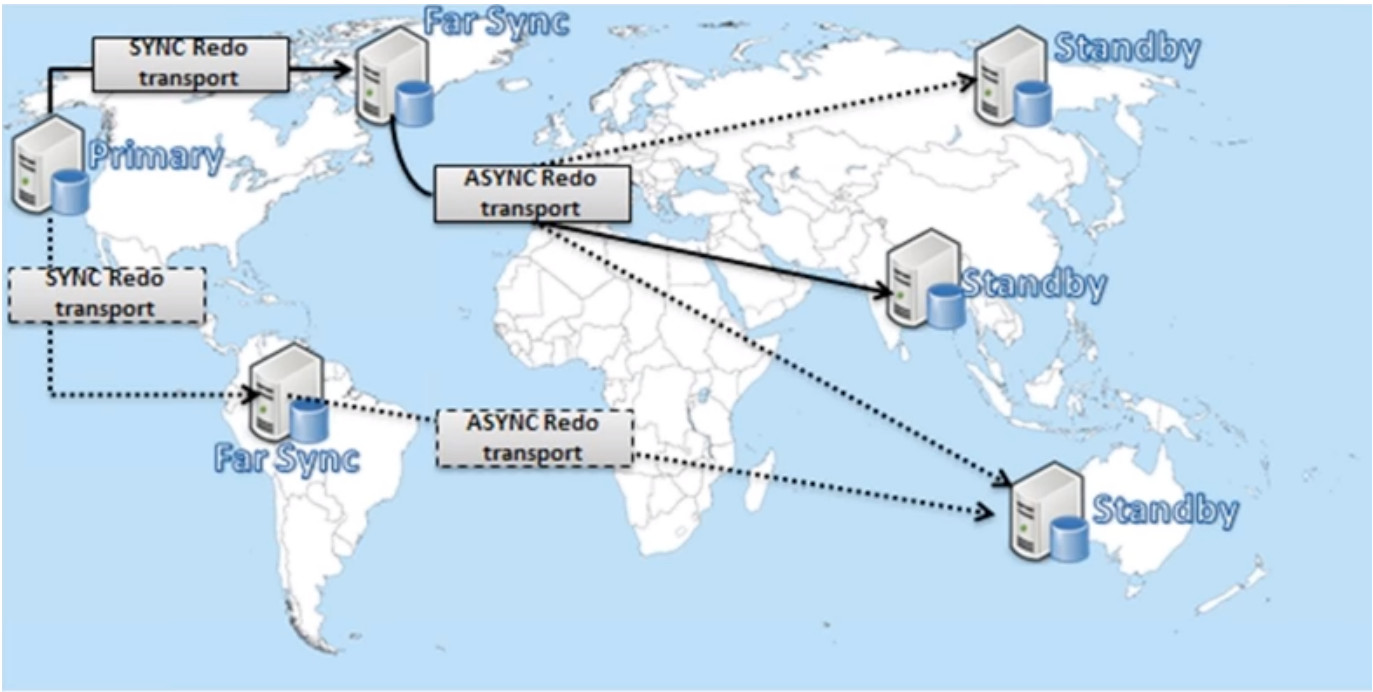
  Contains the same logical information as the production database, although the physical organization and structure of the data can be different.

- **Snapshot Standby Database (Redo data apply)**

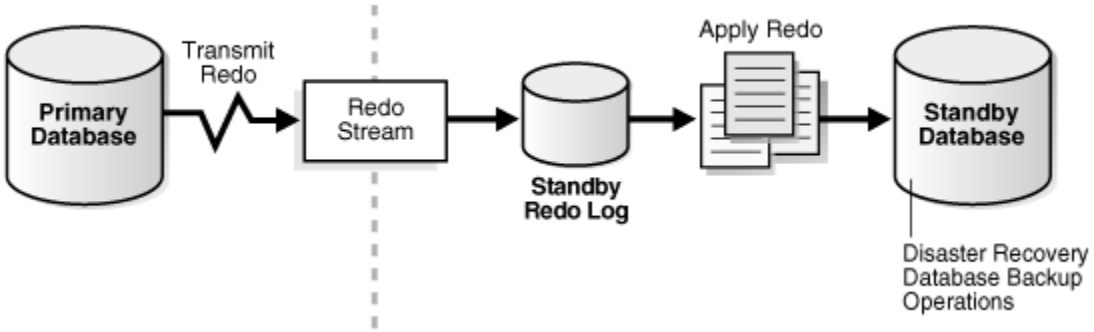
Like a physical or logical standby database, a snapshot standby database receives and archives redo data from a primary database. Unlike a physical or logical standby database, a snapshot standby database does not apply the redo data that it receives. The redo data received by a snapshot standby database is not applied until the snapshot standby is converted back into a physical standby database, after first discarding any local updates made to the snapshot standby database.

2.1.3 Far Sync Instances

An Oracle Data Guard far sync instance is a remote Oracle Data Guard destination that accepts redo from the primary database and then ships that redo to other members of the Oracle Data Guard configuration.



2.1.4 Configuration Example



2.2 Oracle Data Guard Services

2.2.1 Redo Transport Services

- Transmit redo data from the primary system to the standby systems in the configuration

- Manage the process of resolving any gaps in the archived redo log files due to a network failure
- Automatically detect missing or corrupted archived redo log files on a standby system and automatically retrieve replacement archived redo log files from the primary database or another standby database

2.2.2 Apply Services

Redo data is applied directly from standby redo log files as they are filled using real-time apply. If standby redo log files are not configured, then redo data must first be archived at the standby database before it is applied.

The main difference between physical and logical standby databases is the manner in which apply services apply the archived redo data:

Redo data apply vs SQL apply.

2.2.3 Role Transitions

Change the role of a database from a standby database to a primary database, or from a primary database to a standby database using either a **switchover** or a failover operation.

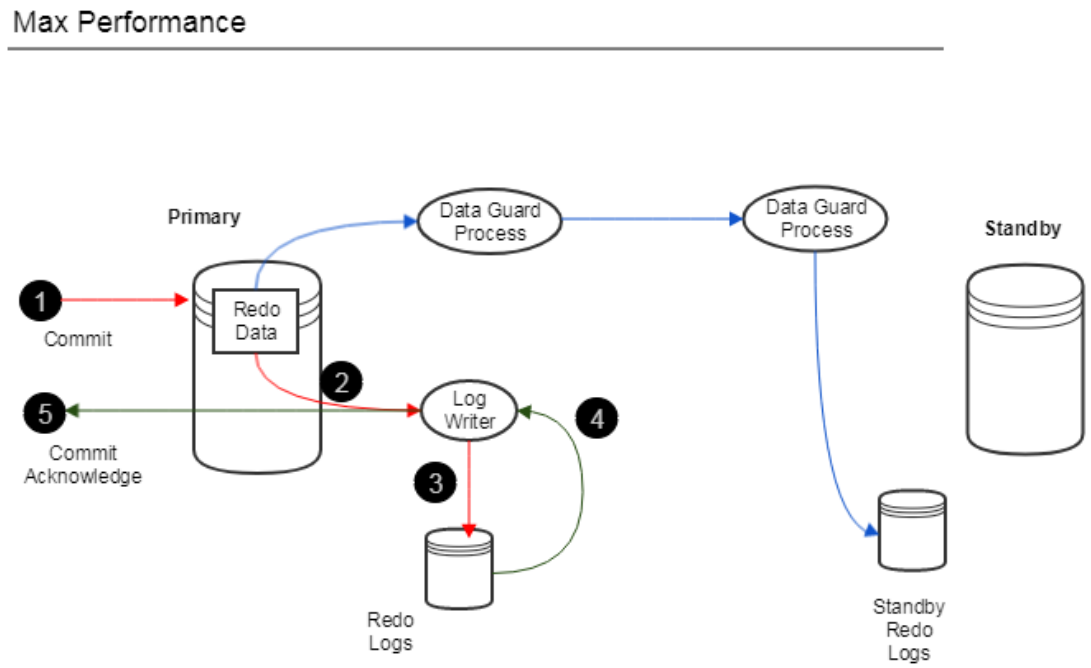
A **switchover** is a role reversal between the primary database and one of its standby databases. A switchover ensures no data loss. This is typically done for planned maintenance of the primary system. During a switchover, the primary database transitions to a standby role, and the standby database transitions to the primary role.

A **failover** is when the primary database is unavailable. Failover is performed only in the event of a failure of the primary database, and the failover results in a transition of a standby database to the primary role. The database administrator can configure Oracle Data Guard to ensure no data loss.

The role transitions described in this documentation are invoked manually using SQL statements. You can also use the Oracle Data Guard broker to simplify role transitions and automate failovers using Oracle Enterprise Manager Cloud Control or the DGMGRL command-line interface, as described in Oracle Data Guard Broker.

2.3 Oracle Data Guard Protection Modes

- **Maximum Performance**

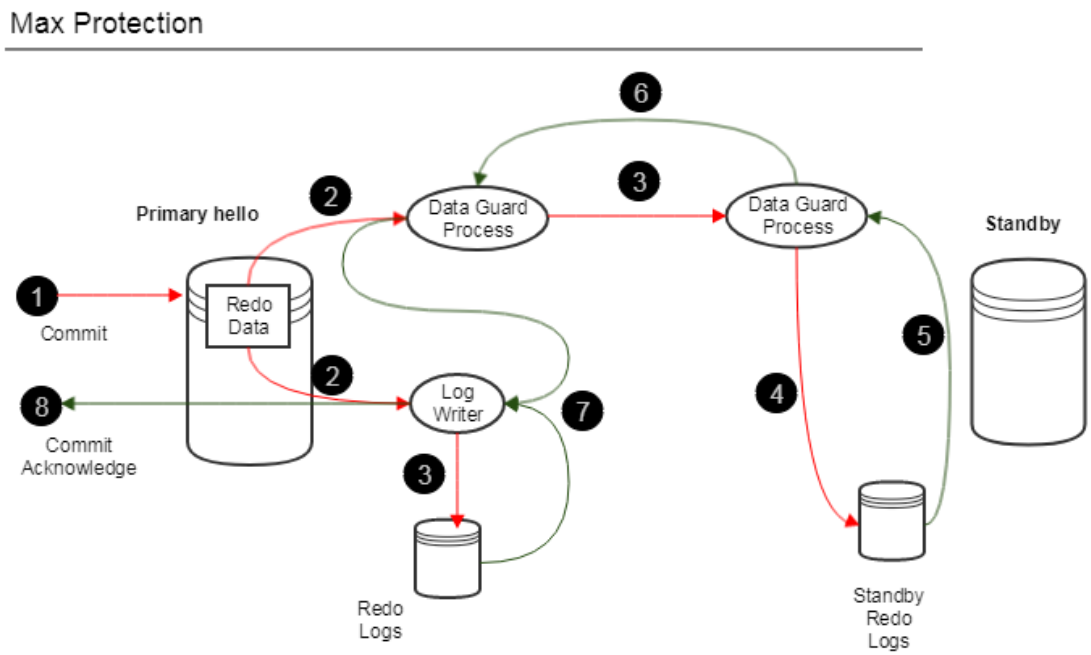


This is the default protection mode. It provides the highest level of data protection that is possible without affecting the performance of a primary database. This is accomplished by allowing transactions to commit as soon as all redo data generated by those transactions has been written to the online log. Redo data is also written to one or more standby databases, but this is done asynchronously with respect to transaction commitment, so primary database performance is unaffected by delays in writing redo data to the standby database(s).

This protection mode offers slightly less data protection than maximum availability mode and has minimal impact on primary database

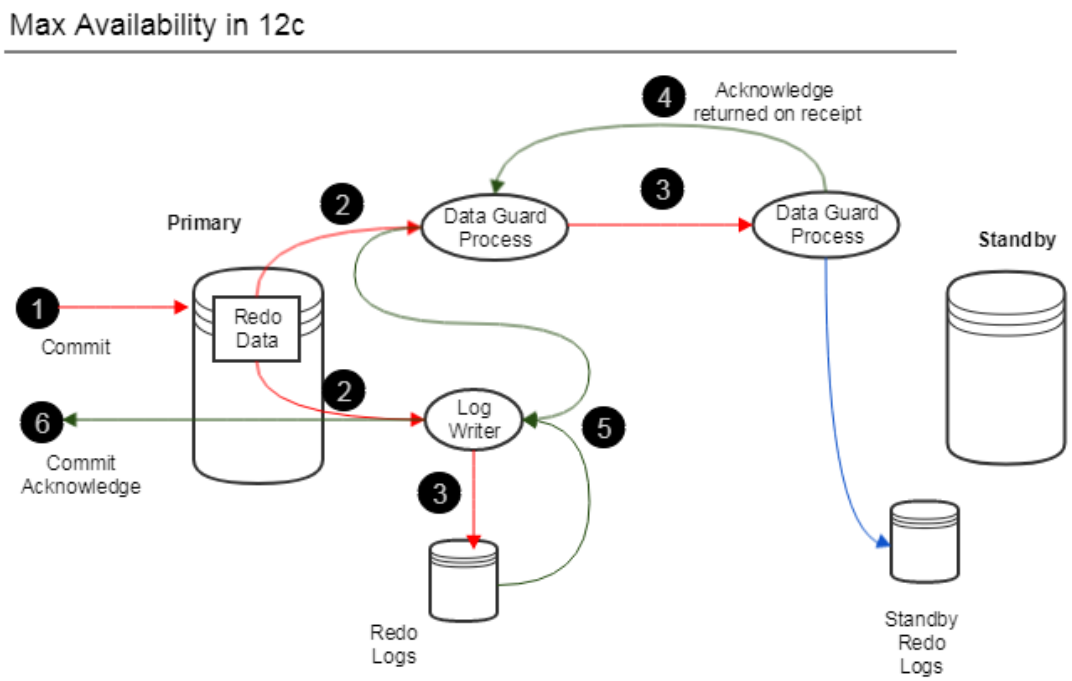
performance.

- **Maximum Protection**



This protection mode ensures that no data loss occurs if the primary database fails. To provide this level of protection, the redo data needed to recover a transaction must be written to both the online redo log and to the standby redo log on at least one synchronized standby database before the transaction commits. To ensure that data loss cannot occur, the primary database shuts down, rather than continue processing transactions, if it cannot write its redo stream to at least one synchronized standby database.

- **Maximum Availability**



This protection mode provides the highest level of data protection that is possible without compromising the availability of a primary database. With Oracle Data Guard, transactions do not commit until all redo data needed to recover those transactions has either been received in memory or written to the standby redo log (depending upon configuration) on at least one synchronized standby database. **If**

the primary database cannot write its redo stream to at least one synchronized standby database, it operates as if it were in maximum performance mode to preserve primary database availability until it is again able to write its redo stream to a synchronized standby database.

This protection mode ensures zero data loss except in the case of certain double faults, such as failure of a primary database after failure of the standby database.

All three protection modes require that specific redo transport options be used to send redo data to at least one standby database.

2.4 Client Failover

Client failover encompasses failure notification, stale connection cleanup, and transparent reconnection to the new primary database. Oracle Database provides the capability to integrate database failover with failover procedures that automatically redirect clients to a new primary database within seconds of a database failover.