B Technical Comparison of DB2 HADR with Oracle Data Guard for Database Disaster Recovery

Oracle Data Guard is a feature of 10g Enterprise Edition that allows for the creation of standby databases that can be kept transactionally consistent with a primary database. To achieve this, Oracle ships log buffers (or log files in some configurations) from the primary server to the standby server where the log records are replayed on the standby database. A Data Guard standby comes in two "flavors": logical standby and physical standby. In logical standby mode, log records are converted to SQL statements and replayed on the standby database. This more closely resembles DB2's SQL Replication and Q Replication capabilities and as such will not be discussed here. In physical standby mode, log records are applied using redo logic, which applies the records much in the same fashion as would occur when rolling forward a database through log files.

In this mode, both the primary and standby databases are exact physical copies of each other and the application of log buffers is similar to that of IBM's HADR. However, there are many differences that appear when you look just below the surface that make HADR a superior solution to Data Guard for high-availability scenarios. A summary of the differences, each of which will be described in detail, follows.

Both IBM's HADR and Oracle's Data Guard protect from failures, such as software failure, primary server failure, storage failure, or even primary site failure. In both cases the configuration can include a second complete copy of the database in a remote location to protect from any or all of these forms of failure. It should be noted that Oracle Real Application Cluster (RAC) only protects from server and software failure on a node in the cluster and has no protection for storage or site failure. To cover more fail-

Note: Used with permission from Chris Eaton.

ure scenarios, Oracle would likely recommend a combination of both Oracle RAC and Data Guard, though the user should be cautious of the increased cost of the solution.

IBM HADR allows for fix packs (patch sets) and OS level fixes to be applied in a rolling fashion. For example, the following steps can be deployed to maintain maximum availability while patches are applied:

1. Stop HADR on the standby.
2. Apply the DB2 fix or OS fix on the standby.
3. Start HADR on the standby—database will automatically resynchronize.
4. Perform a switch-roles takeover.
5. Stop HADR on the new standby (old primary).
6. Apply the DB2 fix or OS fix to this server.
7. Start HADR on the new standby (old primary)—database will automatically resynchronize.

At this point, since HADR is intended to be a peer-to-peer HA solution, you can leave the roles as they are above. Alternatively, you can perform a takeover to switch roles again to get back to the original primary/standby configuration. With Oracle Data Guard, a physical standby database does not support rolling upgrades. Both primary and standby servers must be using the same patch set.

B.1 Standby Remains "Hot" during Failover

The following sequence of events occurs on the standby during an HADR takeover:

1. Last log buffer is replayed (if not already done).
2. Undo of in-flight transactions occurs—note that the buffer pool on the standby is likely full of all the recent updates so there is likely little to no random data page I/O during undo recovery.
3. New transactions are allowed to access the database. Note that the buffer pool and all other memory structures remain allocated.

With Data Guard, in order to convert a standby into a primary (during either failover or when switching roles) the standby database must be shutdown and started up again. This results in buffer caches, catalog caches, and package caches (library caches) being torn down and recreated. Therefore, a significant "brown out" period would follow a Data Guard failover. According to a presentation given by Angelo Pruscino, Principal Architect, Oracle Corporation, there is an issue with warming the buffer cache on a cold failover that can take "5+ minutes" to resolve.

B.2 Subminute Failover

HADR has been demonstrated with a failover of a database supporting 600 concurrent SAP users and was achieved in only 11 seconds. Clearly HADR is capable of supporting subminute failover.

One of the issues with Data Guard is that you must stop and restart the instance during failover, which negatively impacts availability. The following quote is from a case study on Oracle's own internal processing systems, which use Data Guard. It is significant to note that this system does not deliver subminute failover.

B.3 Geographically Separated

Both HADR and Data Guard use TCP/IP to send log buffers from the primary server to the standby site. As such, both allow for the servers to be separated by a large distance. In addition, both products offer asynchronous buffer transmission so that very large distances do not adversely affect the performance of the primary server.

B.4 Support for Multiple Standby Servers

With the first release of HADR, DB2 supports one primary and one standby database. The key objective is to provide the highest levels of availability possible. An issue with multiple standby servers is that the impact on the primary server becomes too great to efficiently support synchronous mode. Therefore, in order to support multiple standby servers, the use of asynchronous mode is more appropriate. IBM's solution for asynchronous multisite standby servers is Q Replication, with which you can have multiple targets for a given source database. The tradeoff to consider when looking at asynchronous modes to multiple standby servers is the potential transaction loss in comparison to HADR in synchronous or near-synchronous modes.

B.5 Support for Read on the Standby Server

Oracle Data Guard allows for the log replay to be suspended on the standby server so that the database can be opened in read-only mode. This, however, elongates the failover times as the standby server cannot be both in read-only mode and be replaying logs at the same time. In some reports, delaying the log apply can add 15 minutes to the failover times. If read on standby is a higher priority, then DB2 Q Replication would be a better alternative. Q Replication allows for read and write on the remote databases. Combined with automatic client reroute, this solution provides "instant" failover as there is no need to recover in-flight transactions after a failover.

B.6 Primary Can Be Easily Reintegrated after Failover

In the event of a failure on the primary server, the standby server can be forced into the primary role. With DB2, the command is called "takeover by force," in which the standby does not need to communicate with the primary prior to taking over the role as the primary database. With DB2 it is possible to reintegrate the old primary into the cluster as a standby. When in synchronous (SYNC) mode, DB2 ensures that the logs on both servers are identical so reintegration only requires an HADR start command on the old primary in order for it to become the new standby. In the case of NEARSYNC, the only possible loss of transaction is if the primary and standby fail simultaneously. If this is not the case then a simple HADR start on the old primary will reintegrate that server as a new standby.

In the case of ASYNC, there is the possibility that the failover to the standby occurred before log records made it to the database on that server. However, it is still recommended that the HADR start command be issued on the old primary after that server comes back up. DB2 will automatically check the log streams on both sites to determine if there were any transactions lost. If no transactions are missing, the old primary will automatically be reintegrated as a standby. If there are missing transactions, IBM Recovery Expert can be used to list the missing transactions and the new standby can be rebuilt from a backup of the new primary. In Oracle Data Guard, a failover requires the original primary to be rebuilt, which adds additional work and elongates the time required to revert back to the original primary server. Following is a quote from the 10gR1 Data Guard Concepts and Administration manual:

> During failovers involving a physical standby database: In all cases, after a failover, the original primary database can no longer participate in the Data Guard configuration. To reuse the old primary database in the new configuration, you must recreate it as a standby database using a backup copy of the new primary database.