Oracle Maximum
Availability Architecture

Disaster Recovery for Oracle Database

Zero Data Loss Recovery Appliance, Active Data Guard and Oracle GoldenGate

ORACLE WHITE PAPER | APRIL 2015

Overview

Oracle Database provides three different approaches to disaster recovery that provide the highest level of data protection and availability compared to any other approach for protecting Oracle data.

Oracle Zero Data Loss Recovery Appliance is an engineered system designed to eliminate data loss and dramatically reduce data protection overhead for all Oracle databases in the enterprise. Integrated with Recovery Manager (RMAN), it enables a centralized, incremental forever backup strategy for hundreds to thousands of databases, using cloud-scale, fully fault-tolerant hardware and storage. Replication capabilities integrated with the Recovery Appliance make it ideally suited for providing disaster recovery for Oracle databases where a restore from backup is sufficient to address recovery time objectives.

Oracle Active Data Guard is the replication solution optimized for data protection and disaster recovery for the Oracle Database. Active Data Guard prevents data loss and downtime by maintaining a synchronized physical replica of the production database. If the production database becomes unavailable for any reason, client connections can quickly, and in some configurations transparently, fail over to the replica to immediately restore service. Active Data Guard also eliminates idle redundancy by allowing read-only workloads to be offloaded to a copy of the production database. Active Data Guard is ideally suited for providing disaster recovery for databases with recovery time objectives that cannot tolerate the downtime that accompanies a restore from backup.

Oracle GoldenGate is Oracle's full-featured replication solution designed to address a wide range of requirements. GoldenGate maintains a synchronized logical copy of a production database that is open read-write at all times. A GoldenGate replica, for example, can offload reporting applications that require read-write database access or can be used to load-balance read-write workloads using multimaster replication. Increased flexibility, however, is accompanied by several trade-offs for data protection and operational simplicity compared to Active Data Guard. GoldenGate is used for disaster recovery by customers who accept these trade-offs in return for its additional flexibility.

This paper provides Oracle Maximum Availability Architecture[1] best practices for the use of the Recovery Appliance, Active Data Guard, and Oracle GoldenGate for disaster recovery. It assumes the reader already has a basic technical knowledge of each solution.

1 http://www.oracle.com/technetwork/database/features/availability/maa-096107.html

Introduction

The Zero Data Loss Recovery Appliance[2] is the Oracle optimized solution for backup and recovery. The Recovery Appliance fundamentally changes how backup and recovery is performed by enabling incremental forever backups and efficient any point-in-time restore. No other backup and recovery solution can match the Recovery Appliance in terms of data protection, operational and system resource efficiency, its ability to scale, and its unique level of backup validation that ensures successful recovery.

The Recovery Appliance is also used for disaster recovery when recovery time objectives (maximum allowable downtime) can be satisfied by a restore from backup and recovery point objectives (maximum allowable data loss) can be satisfied by the appliance's replication capabilities.

Active Data Guard[3] is the real-time data protection and availability solution for the Oracle Database. It is the Oracle solution for maintaining a synchronized, hot copy of an Oracle Database at a remote location for disaster recovery. Active Data Guard is differentiated from the Recovery Appliance by its ability to provide an already running replica that can immediately resume a full level of service should an outage occur – no restore required. Active Data Guard also performs an additional level of continuous data validation and automatic corruption repair that results in high availability (HA).

Oracle GoldenGate[4] is a very flexible logical replication solution that may be used in place of Active Data Guard to maintain a synchronized copy of a production database for disaster recovery. GoldenGate's increased flexibility, however, is accompanied by several trade-offs for data protection and operational simplicity compared to Active Data Guard. GoldenGate may be used for disaster recovery by customers who accept these trade-offs in return for the additional flexibility of logical replication and who wish to deploy a single replication solution.

Active Data Guard or GoldenGate are used for disaster recovery when fast recovery times or additional levels of data protection are required. The Recovery Appliance still plays a substantial role in any configuration where Active Data Guard or GoldenGate are used by providing the complementary functions of backup and recovery, and archival to tape.

Note: Active Data Guard is a separately licensed option for the Oracle Database. It provides advanced capabilities for data protection, availability and production offload of read-only workloads and backups. Active Data Guard is an extension of basic Data Guard capabilities included with Oracle Database Enterprise Edition. This paper will describe a capability as an Active Data Guard feature if it requires an Active Data Guard license. Capabilities included with Data Guard in Oracle Enterprise Edition will be described as Data Guard capabilities. By default, every Data Guard capability is also part of Active Data Guard.

Oracle MAA Reference Architectures

Oracle MAA best practices describe four HA reference architectures that address the complete range of requirements for data protection and availability, including disaster recovery, typical for enterprises of all sizes and markets[5]. The architectures, or HA tiers, are designated PLATINUM, GOLD, SILVER, and BRONZE. They deliver the following service levels:

2 https://www.oracle.com/engineered-systems/zero-data-loss-recovery-appliance/index.html

3 http://www.oracle.com/technetwork/database/options/active-data-guard/overview/index.html

4 http://www.oracle.com/technetwork/middleware/goldengate/overview/index.html

5 http://www.oracle.com/technetwork/database/availability/maa-reference-architectures-2244929.pdf

» Platinum: Zero application outage for Platinum-ready applications. Zero data loss protection (data loss potential = zero) for all non-recoverable outages, including disasters that impact a large geography.

» Gold: HA for all outages: server, database, cluster, site, and region. Fast failover with options for zero data loss or near-zero data loss disaster protection.

» Silver: HA for recoverable outages within a data center. Continuous real-time backup with any-point in time restore that provides near-zero data loss protection from unrecoverable outages and disasters.

» Bronze: Basic service restart for recoverable outages. Database integrated corruption protection and backups with any-point-in-time restore to protect data from unrecoverable outages and disasters.

Each tier uses a different MAA reference architecture to deploy the optimal set of Oracle HA capabilities that reliably achieve the stated service levels at the lowest cost and complexity. They explicitly address all types of unplanned outages including data corruption, component failure, human error, system and site outages, as well as planned outages due to maintenance, migrations, or other purposes. Figure 1 provides a high level overview of the reference architectures.

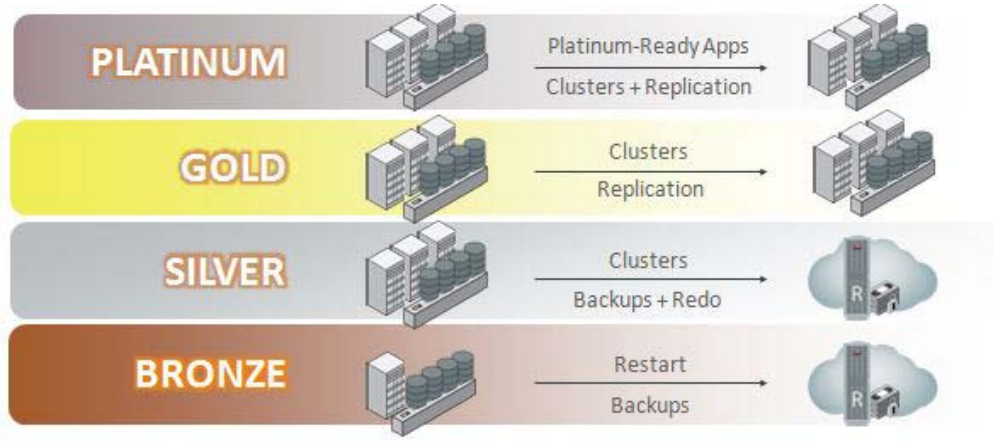

Figure 1: Oracle MAA Reference Architectures

The Recovery Appliance is utilized for disaster recovery in the Bronze and Silver tiers and for backup and recovery in every tier. Database replication, either Active Data Guard or GoldenGate, are used for disaster recovery in the Gold Tier. Active Data Guard is used for disaster recovery in the Platinum tier where both fast recovery time and zero data loss protection are required. The following sections illustrate MAA best practice for each tier.

Bronze Disaster Recovery

MAA best practice for using the Recovery Appliance for disaster recovery at the Bronze tier is depicted in Figure 2. The Bronze tier utilizes a local Recovery Appliance for backup and recovery. The local Recovery Appliance (the upstream appliance) also replicates backups to a second appliance (the downstream appliance) at a remote location for disaster recovery.

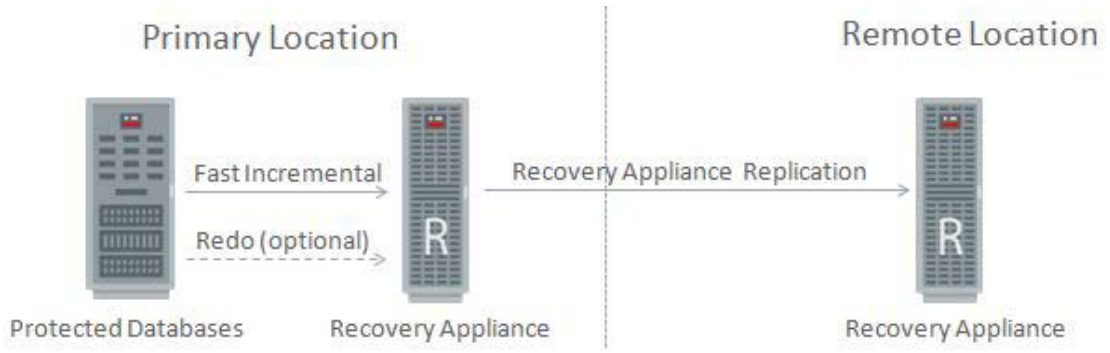

Figure 2: Recovery Appliance and Bronze Reference Architecture

Additional details include:

- The Bronze tier is appropriate for databases having less stringent recovery time and recovery point objectives. Bronze databases, for example, may not be configured for archive log mode and thus accept the risk of losing all data generated since the last full or incremental backup was taken should an unrecoverable outage occur.
- There are cases, however, where customers in the bronze tier require enhanced protection and choose to run in archive log mode to enable archive log backups.
  - Oracle recommends using the real-time redo shipping feature of the Recovery Appliance as the most efficient mechanism to perform archive log backups. Real-time redo is configured between the protected database and the upstream appliance using the same asynchronous transport method as Data Guard.
  - Real-time redo enhances data protection by continuously backing up redo for the most recent transactions.
  - Real-time redo also levels bandwidth consumption between the protected database and the upstream appliance by streaming redo rather than batching the transmission of archive log backups.
  - When the protected database switches online logs, the upstream appliance archives the redo it has received, backs it up, and places the backup in a queue to be replicated to the downstream appliance.
  - Archive log management follows standard RMAN deletion policies set at the protected database.
- The upstream appliance, replicates both backups and archive logs (if any) to the downstream appliance.
  - The recovery point objective (RPO) in a disaster for protected databases not configured for archive log mode is equal to all transactions committed since the last backup replicated to the downstream appliance.
  - RPO in a disaster for protected databases configured for archive log mode with real-time redo shipping is equal to any archive log backups that have not yet been replicated between appliances.
- A third-party network device capable of compressing network traffic is currently the most efficient mechanism to conserve network bandwidth when replicating backups and archive logs (if any) between appliances.
- While not pictured, the upstream and downstream Recovery Appliances can also archive on-disk backups directly to tape at either location. Off-site tape storage is also a viable option for disaster recovery as a lower cost alternative than a downstream appliance – but with substantial tradeoffs in the level of data protection, management, reliability, and recovery time compared to using a Recovery Appliance.

Silver Disaster Recovery

The Silver reference architecture is identical to Bronze except that all protected databases are expected to run in archive log mode and be configured for real-time redo transport for the highest level of data protection, see Figure 3.

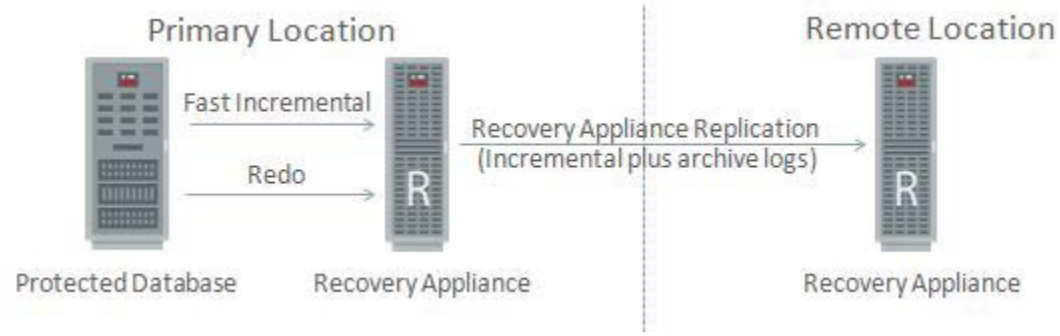

Figure 3: Recovery Appliance and Silver Reference Architecture

Bronze and Silver Disaster Recovery Utilizing a Hub and Spoke Architecture

The Recovery Appliance offers flexible replication topologies that provide customers additional opportunities to reduce cost by centralizing investment in disaster recovery systems and facilities. A hub and spoke architecture shown in Figure 4 is an example of an approach where a central location serves as a hub for all DR services.

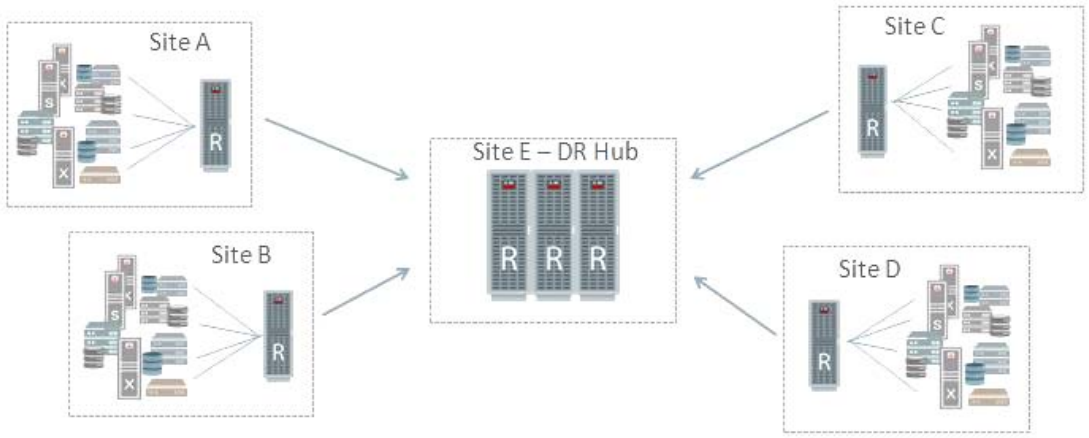

Figure 4: Hub and Spoke Architecture Using Recovery Appliance Replication

Gold Disaster Recovery

The Gold reference architecture uses database replication, either Active Data Guard or Oracle GoldenGate, for disaster recovery to provide enhanced data protection and fast failover that can improve both RPO and recovery time (RTO). The Recovery Appliance continues to perform a complementary role for backup and recovery. Database replication does not eliminate the usual role for backups as a final layer of protection (a last resort for recovery) and for archival purposes.

While either Active Data Guard or GoldenGate can provide disaster recovery, they are very different replication technologies that are optimized for different purposes. Active Data Guard, for example, provides either zero data loss protection using Maximum Availability mode or near-zero data loss protection using Maximum Performance mode. GoldenGate, in contrast, is an inherently asynchronous replication process that does not have the equivalent of Active Data Guard zero data loss protection. The following sections provide an overview of the different considerations that apply to each.

Active Data Guard

A high-level depiction of the Gold reference architecture using Active Data Guard is provided in Figure 5. Additional details include:

- Data Guard Maximum Availability mode combined with synchronous redo transport is the general recommendation for the Gold reference architecture to provide zero data loss protection. The DR RPO is zero when using Data Guard Maximum Availability.
  - Users should consider using Active Data Guard Far Sync with Oracle Database 12c when zero data loss protection is required and there is a concern for the impact of round-trip network latency on production database performance. Far Sync is described later in this paper.
- Data Guard asynchronous transport with Maximum Performance mode is acceptable if the performance impact of round-trip network latency between primary and standby locations is too great to support synchronous transport and service levels can tolerate data loss should an unrecoverable outage occur. DR RPO is measured in single-digit seconds when using Data Guard Maximum Performance assuming there is sufficient network bandwidth provided to handle peak redo volume.

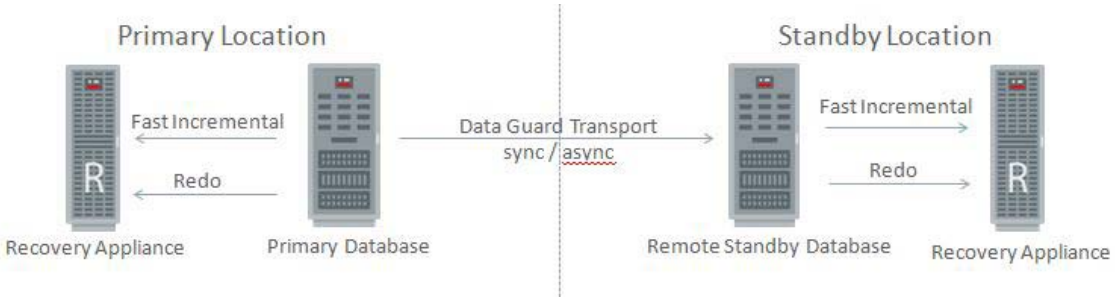

Figure 5: Active Data Guard and Recovery Appliance – Gold Reference Architecture

- Active Data Guard automatic block repair will detect and repair physical block corruption should they be encountered at either the primary or the standby database, transparent to the application.

- Data Guard lost-write detection is enabled at both the primary and standby to provide automatic detection of silent corruptions caused by misdirected or lost writes due to lower level faults in the I/O path. Additional real-time Oracle data validation checks for both physical data corruption and logical intra-block data corruption should be configured following best practices described in My Oracle Support Note 1302539.1, *"Best Practices for Corruption Detection, Prevention, and Automatic Repair"*.
- A Recovery Appliance is deployed in each location to perform local backups of their respective primary or standby databases.
  - Fast incremental backups are taken using RMAN block-change tracking from both the primary and the Active Data Guard standby.
  - Primary and standby databases are each configured for real-time redo shipping to their local Recovery Appliance. Standby databases are configured to cascade redo received from the primary.

Note: Active Data Guard with Oracle Database 12c enables redo to be cascaded in real-time as it is received from the primary database. Basic Data Guard standby databases cascade redo upon a primary log switch.

  - A single Data Guard redo stream is the only data that must be transmitted between sites to maintain both a synchronized remote standby and a remote backup.
  - Backups taken by either appliance can be used to restore any database in a Data Guard configuration due to the fact that a Data Guard standby database is a physical replica of production.
  - The only time a backup would need to be copied or replicated across the wide area network is if a local Recovery Appliance is unavailable when needed to perform backup or recovery.
- Archive log management follows the standard RMAN deletion policies set at the primary and standby database.

Oracle GoldenGate

Oracle GoldenGate is a very flexible logical replication solution commonly used for advanced replication requirements such as multimaster replication, subset replication, data integration, many-to-one replication, zero downtime maintenance and migrations, data transformation, etc. It is also a replication solution that may be used in place of Active Data Guard to maintain a synchronized copy of a production database for disaster recovery. GoldenGate's increased flexibility, however, is accompanied by several trade-offs specific to data protection and operational simplicity compared to Active Data Guard. GoldenGate is used for disaster recovery by customers who accept these trade-offs in return for the additional flexibility of logical replication and who prefer to deploy a single replication solution.

Note that there are many cases where customers deploy both Active Data Guard and Oracle GoldenGate in the same configuration for optimal benefit across multiple use-cases. For example, an Oracle GoldenGate source database replicates subsets of data to multiple targets for data distribution or data integration purposes. The GoldenGate source is also protected by an Active Data Guard standby database for disaster recovery. Oracle MAA best practices are utilized so that when there is an Active Data Guard failover or switchover, GoldenGate replication automatically restarts on the new primary database and picks up right where it left off when the outage occurred.[6]

6 http://www.oracle.com/technetwork/database/availability/ogg-adg-2422372.pdf

A GoldenGate configuration for the Gold reference architecture used in place of Active Data Guard looks similar to that shown in Figure 5, but with the following special considerations:

- All databases must meet prerequisites for logical replication described in the GoldenGate documentation.
- GoldenGate is an inherently asynchronous replication process; it has no equivalent of Data Guard Maximum Availability for zero data loss protection and thus is unable to guarantee a zero RPO. A GoldenGate source database requires its own Data Guard standby for zero data loss protection from unrecoverable outages. In a GoldenGate mulitmaster configuration, each copy requires its own Active Data Guard standby for zero data loss protection since each copy is also a source database.
- Source and target databases are logical, not physical copies of each other. This means that while each copy may contain the same data, their physical structures are different. It is also possible for each copy to have unique local tables and indexes that do not exist in the other. This results in the following:
  - GoldenGate has no equivalent of Active Data Guard Automatic Block Repair. Physical corruptions that cannot be automatically repaired by Automatic Storage Management (ASM) or storage mirroring using a locally mirrored copy will cause transactions to fail and require manual intervention to repair.
  - GoldenGate has no equivalent of Data Guard lost-write detection. GoldenGate cannot offload the overhead of lost-write detection from the production database, nor can it detect lost-write corruptions that can occur independently in a source or target database.
  - Backups are not interchangeable between GoldenGate source and targets, each is a different database. Users who wish to maintain a remote backup for each database must replicate Recovery Appliance backups and archive logs over the wide area network in addition to data replicated by GoldenGate.
- Depending upon workload, there may be additional performance considerations when using logical replication compared to physical database replication performed by Active Data Guard.

Platinum Disaster Recovery

The Platinum reference architecture is similar to Figure 5 and differs from Gold in that it standardizes upon Active Data Guard for disaster recovery due to the requirement for zero data loss protection for unrecoverable outages.

GoldenGate complements Active Data Guard by enabling zero-downtime planned maintenance. GoldenGate bi-directional replication is used to maintain synchronize between the existing database environment and a parallel environment having its own primary and Active Data Guard standby operating at the new release. After the new release is validated, users are gradually migrated as they naturally disconnect and then reconnect – providing a zero downtime upgrade experience. GoldenGate replication along with the environment running at the previous release is decommissioned after all users have migrated and there is no longer the need for fast fallback. The complementary use of Active Data Guard and GoldenGate in this manner provides both zero downtime upgrade and zero data loss protection with immediate failover should an unplanned outage occur at any time during the upgrade process.

Additional details for Platinum disaster recovery include:

- DR RPO is zero using Data Guard Maximum Availability combined with synchronous redo transport. This eliminates data loss in the event of unrecoverable outages of the primary database.
- Active Data Guard Far Sync with Oracle Database 12c (described in the next section of this paper), is used if there is a concern for the impact of round-trip network latency on production database performance.
- Data Guard Fast-Start Failover provides an option for automating database failover to further improve RTO for the Oracle Database. For optimal transparency at the application tier during database outages, consider deploying a second standby database local to the primary as described later in this paper. This can enable the existing

application tier to automatically switch between primary and standby databases during unplanned outages or planned maintenance without forcing a restart of the application tier or requiring users to reconnect[7].

» In contrast to unplanned outages, the planned switchover of production between a GoldenGate source and target is always a zero data loss event. This combined with bi-directional replication makes GoldenGate the ideal complement to Active Data Guard for zero downtime planned maintenance.

Gold and Platinum Option 1: Active Data Guard Far Sync

Active Data Guard Far Sync is a new capability with Oracle Database 12c that enables zero data loss protection at any distance by preventing WAN network latency from impacting production database performance.

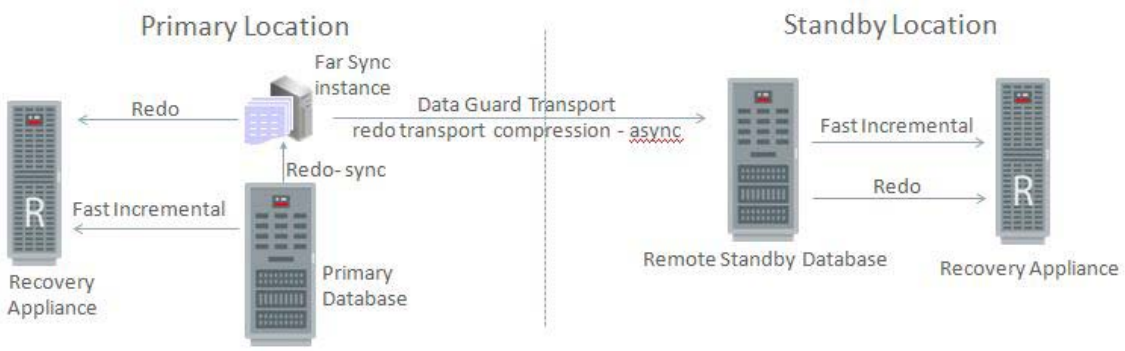

Figure 6: Zero Data Loss Failover at Any Distance Using Active Data Guard Far Sync

Far Sync, described in Figure 6, enables zero data loss failover to a remote standby database regardless of distance by deploying a Far Sync instance that has the following characteristics:

» A Far Sync instance is a lightweight Oracle instance that has only a control file, spfile, password file, and standby log files; there are no database files or online redo logs.

» The Far Sync instance is deployed at a distance that is within an acceptable range of the primary for synchronous redo transport (generally less than 5ms round-trip network latency. The remote standby database may be deployed at any distance from the Far Sync instance.

» A Far Sync instance receives redo from the primary via Data Guard synchronous transport and immediately forwards the redo to up to 29 remote standby databases via asynchronous transport.

» A Far Sync instance can also forward redo to a Recovery Appliance. A primary database that is protected by both a Recovery Appliance and a remote standby database need only ship a single redo stream and the Far Sync instance will distribute the redo to multiple destinations.

» The presence of a Far Sync instance in a Data Guard configuration is transparent to its operation during switchover or failover; the administrator uses the same commands used for any Data Guard configuration. Automatic database failover also operates in an identical fashion.

Additional details for this option include:

» The DR RPO using the remote standby database is zero.

7 http://www.oracle.com/technetwork/database/availability/client-failover-2280805.pdf

» The Far Sync instance can compress the redo it transmits over the WAN to conserve network bandwidth by using Data Guard redo transport compression (this requires the primary and standby databases be licensed for Oracle Advanced Compression).

» The remote standby database is configured to cascade redo to the downstream recovery appliance.

» Archive log management follows the standard RMAN deletion policies set at the primary, standby, and Far Sync instance.

Gold and Platinum Option 2: Multi-standby

It is increasingly common to see customers with stringent requirements for high availability and disaster recovery utilize configurations with multiple synchronized replicas of the production database as illustrated in Figure 7.

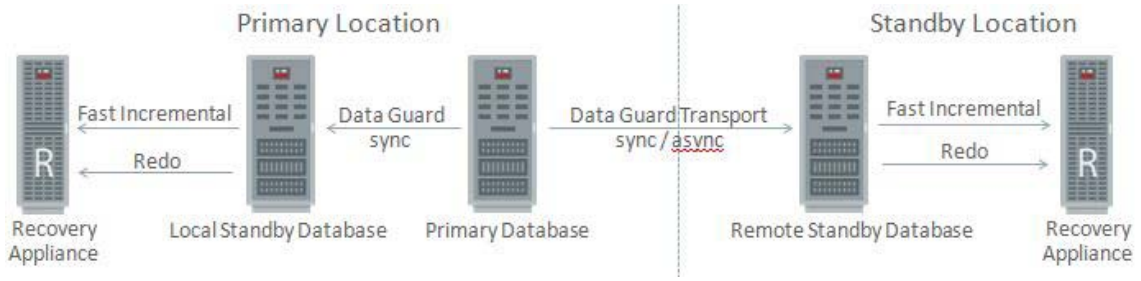

Figure 7: Multi-Standby Configuration with Local HA Failover

Additional details for the configuration described in Figure 7 include:

» The primary database transmits redo either asynchronously or synchronously, directly to both local and remote standby databases. Alternatively, a Far Sync instance can be used to enable the primary to ship once, and allow the Far Sync instance to distribute redo to all other destinations. All of the same benefits and characteristics of Far Sync described in the previous section apply.

» Synchronous transport between the primary database and the local standby is simple to support due to low network latency. This enables the local standby to provide HA-failover should any event impact the availability of the primary database but leave the application tier intact. Upon failure, the application tier receives notification that a database failover has occurred, immediately drops dead connections, and automatically reconnects to the services now available at the new primary database.[8]

» Following a failover to the local standby, the remote standby database automatically recognizes that failover has occurred and begins receiving redo from the new primary database - maintaining DR protection at all times.

» Both local and remote standby databases cascade redo to their respective recovery appliances.

» Archive log management follows the standard RMAN deletion policies set at the primary and standby.

» The local standby database can be multi-purposed to offload read-only workloads from the primary database using Active Data Guard, to offload fast incremental backups using Active Data Guard, to function as a test system using Data Guard Snapshot Standby, or to perform database rolling upgrades.

8 http://www.oracle.com/technetwork/database/availability/client-failover-2280805.pdf

Conclusion

Oracle Database-integrated disaster recovery solutions provide the highest level of data protection and availability compared to any other approach for protecting Oracle data.

The Recovery Appliance is used for disaster recovery when recovery time objectives (maximum allowable downtime) can be satisfied by a restore from backup and recovery point objectives (maximum allowable data loss) can be satisfied by the appliance's replication capabilities. No other backup and recovery solution can match the Recovery Appliance in terms of data protection, operational and system resource efficiency, its ability to scale, and its unique level of backup validation that ensures successful recovery.

Active Data Guard is used for disaster recovery when fast recovery and/or maximum levels of data protection are required. Active Data Guard is optimized for real-time data protection, availability and disaster recovery for the Oracle Database.

Oracle GoldenGate is used for disaster recovery when users require the added flexibility and advanced capabilities of a full-featured logical replication solution.

In every case where a database replication solution is used for disaster recovery, the Recovery Appliance still plays a critical role by providing the complementary functions of enterprise-scale backup, any-point in time recovery, archival to tape, and more.

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle
oracle.com

Hardware and Software, Engineered to Work Together