

Reality Resilience Features

Introduction

Data in a database constitutes a substantial financial investment and will often contain commercially or socially sensitive information. Reality provides a wide range of cost effective options to maximize availability, including Transaction Handling and Logging, Shadow Database and a Rapid Recovery File System. Multiple Systems offer Failsafe operation, auto user-switchover with Heartbeat and remote recovery with Disaster Recovery features.

FailSafe Software

FailSafe software provides a high-level of resilience by maintaining identical databases on separate systems. This reduces loss of service and data in the event of system failure. Users log on to the 'primary' live database with a secondary system and database maintained as a standby. Updates performed on the primary are automatically copied to the secondary as they occur. If the live database fails the secondary can be re-configured as the live database. Service is thereby maintained with minimal interruption.

Maintaining Service: FailSafe supports all of the data security features of Transaction Logging, with the added facility of a standby system and database in case of failure.

For additional security disk logging is performed on both primary and secondary databases and the respective systems each have a dedicated logging disk.

Re-synchronization after database failure can be attained without interrupting service on the live database.

FailSafe Configuration: FailSafe databases, primary and secondary, are configured on separate machines connected to each other via a Local Area Network. In order to transfer the substantial volume of changes made by a modern application, FailSafe systems use a dedicated link between primary and secondary databases for optimum efficiency. Both symmetric and asymmetric sized systems can be configured in FailSafe mode. A symmetric configuration consists of two systems of equal size. An asymmetric configuration consists of two systems, one larger than the other with the larger one normally supporting the primary database. In this case the smaller system must be large enough to support the required minimum user workload of the database.

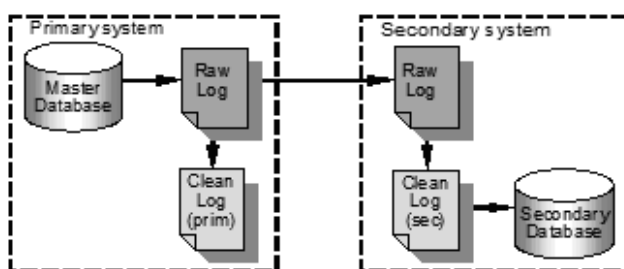
Online Maintenance: FailSafe allows suspension of secondary database update. This enables file-saves, software or hardware upgrades and general maintenance on the secondary while the primary remains live and unaffected.

Reality Disaster Recovery

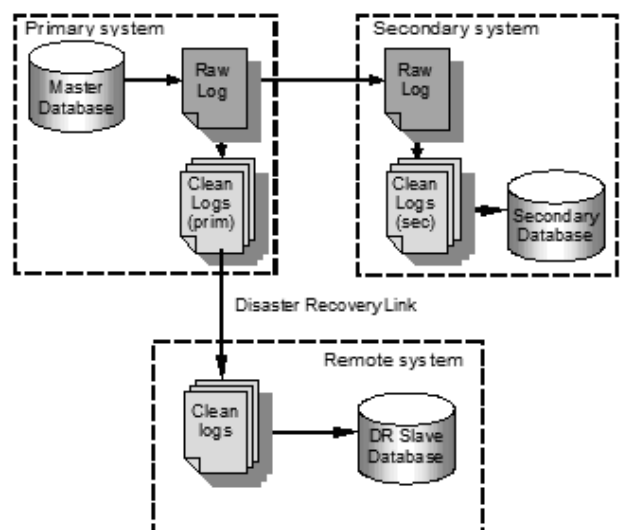
The Reality Disaster Recovery (Reality DR) feature compliments other resilience features by maintaining a database copy on a remote system, via possibly slow or intermittent communication links.

This allows for offsite replication of a standalone system that can form part of the contingency that meets the requirements of ISO 17799:2005 Information Security Standard.

FailSafe



Reality Disaster Recovery



Resilience Features

Reality DR can also increase the resilience of Failsafe systems by providing a second backup system, which would normally be offsite. This has two advantages; Firstly, if the secondary system is taken down for maintenance purposes, you will remain protected against failure of the primary system. Secondly, in a disaster situation where the computer facility is destroyed, both the primary and secondary databases may be lost. An offsite backup system ensures that your data remains safe whilst providing a hot standby system.

Transaction Handling

Transaction Handling enables a Reality application to include markers defining transactions. A transaction is a set of related database updates that must be completed indivisibly for the database to remain consistent. If a process fails in mid-transaction, or the transaction is aborted, Transaction Handling reverses all updates made since the start of the transaction and restores the database to its pre-transaction state. It also suspends file lock release during the transaction, in order to prevent corruption due to unwanted interaction between transactions.

Transaction Logging

Transaction Logging enhances the data security and resilience of a Reality database by recording all changes made by both completed transactions and discrete updates (those not defined within a transaction). This enables full recovery of the most recent and consistent version of the database if a system or application fails. Restoring the last database backup, followed by all completed transactions and discrete updates logged since that backup was made, recovers the database.

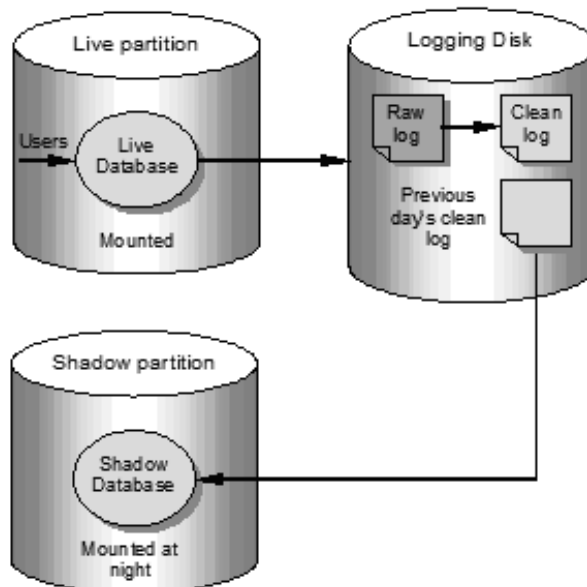
Rapid Recovery

Rapid Recovery records all database structural changes and all updates to files marked as 'recoverable' or 'logged'. This enables the integrity of all files to be restored within minutes of restarting a database after a host platform system failure. Data consistency is restored, where transactions are defined, by deletion of uncompleted transactions. In addition, all updates and complete transactions logged at the point of failure are restored to bring the database up to date. Rapid Recovery can be used together with Transaction Logging to minimize data loss if, for example, a disk subsystem fails.

Shadow Database

Shadow Database enhances resilience by enabling two copies of a database to be maintained on different disk subsystem partitions on a single system. One copy is the 'live' database, to which users log on. A second copy, 'un-mounted' on a separate partition, is referred to as the 'shadow database'.

During routine (typically, daytime) operation the shadow database is unavailable to users. Each night the shadow database is mounted and updates from the day are re-played onto the shadow to resynchronize it with the live database.



Shadow Database

Data Integrity and Security: Shadow Database provides the same data integrity guarantees as Transaction Logging. Transactions and independent updates are logged to clean logs associated with both the live and shadow databases.

Live and shadow databases are maintained on separate disk subsystems and the shadow is maintained un-mounted. The raw and clean log partitions are maintained on another disk mirrored subsystem. This ensures a high level of data security.

If a system or other failure causes the live database to become corrupted, normal database operation can be recovered quickly using the administration utility, which enables the shadow to be mounted, brought up to date, and then made 'live'. This avoids the relatively lengthy procedure of restoring the last FILE-SAVE from tape. The failed database is then restored and re-configured as the shadow without impacting current users.

Database Isolation

Database Isolation makes it possible to run multiple instances of the same version of Reality. Each instance runs completely independently of other instances in much the same way as different versions of Reality, giving two main advantages:

Firstly, Application service providers who host Reality databases for a number of separate customers can run these databases in complete isolation.

Secondly, users on one database are unable to disrupt users on other databases.