Trang lót bìa

**NHẬN XÉT CỦA ĐƠN VỊ THỰC TẬP**

**NHẬN XÉT CỦA GVHD**

**LỜI CẢM ƠN**

**LỜI CAM ĐOAN**

**MỤC LỤC**

Danh mục các chữ viết tắt

Danh mục các bảng biểu

Danh mục hình

LỜI MỞ ĐẦU

**Lý do chọn đề tài**

**Mục đích nghiên cứu**

**Đối tượng và phạm vi nghiên cứu**

**Phương pháp nghiên cứu**

**Bố cục đề tài**

**CHƯƠNG I: TỔNG QUAN**

**1.1 Khái quát về Công ty Tài chính Ngân hàng TMCP Sài Gòn – Hà Nội SHB Finance**

**1.1.1 Giới thiệu chung về SHB Finance**

Công ty Tài chính Ngân hàng TMCP Sài Gòn – Hà Nội SHB Finance là một công ty hoạt động và cung cấp dịch vụ trong lĩnh vực Tài chính tiêu dùng phổ biến cho người dân và doanh nghiệp như cho vay nâng cấp thiết bị, sửa sang nhà cửa, mua xe hơi, du học, chăm sóc sức khỏe, bảo hiểm. “Công ty Tài Chính TNHH Ngân hàng TMCP Sài Gòn - Hà Nội (SHBFinance), được thành lập ngày 12/12/2016 (Mã số doanh nghiệp: 0107779290) với hình thức pháp lý ban đầu là Công ty Tài Chính TNHH MTV Ngân hàng TMCP Sài Gòn - Hà Nội. Ngày 2/6/2023, Ngân hàng Nhà nước Việt Nam đưa ra Quyết định chuyển đổi Công ty Tài chính TNHH MTV Ngân hàng TMCP Sài Gòn – Hà Nội thành Công ty Tài chính TNHH Ngân hàng TMCP Sài Gòn – Hà Nội.”

* Tên công ty: Công ty Tài Chính TNHH Ngân hàng TMCP Sài Gòn - Hà Nội
* Tên tiếng Anh: SHB Consumer Finance Company Limited
* Tên gọi tắt: SHB Finance
* Địa chỉ: Tầng 6, Gelex Tower, 52 Lê Đại Hành, phường Lê Đại Hành, Quận Hai Bà Trưng, Hà Nội
* Điện thoại: 024 7109 8888
* Website: <https://www.shbfinance.com.vn/>
* Logo**:**



Hình 1: Logo thương hiệu công ty SHB Finance

Tiền thân là công ty Tài chính Vinaconex thuộc tập đoàn Viettel, hiện tại công ty hoạt động theo loại hình TNHH từ hai thành viên trở lên. Hiện tại, đang có hai tổ chức sở hữu 50% trên tổng số vốn điều lệ 1000 tỷ mỗi bên là Ngân hàng TMCP Sài Gòn – Hà Nội (SHB) và Ngân hàng TNHH Đại chúng Ayudhya (Krungsri) của Thái Lan. “Ngân hàng Sài Gòn – Hà Nội (SHB) vốn được biết đến thuộc top 5 ngân hàng tư nhân lớn nhất Việt Nam với 30 năm hình thành và phát triển. Tập đoàn tài chính Krungsri có 75 năm hình thành và phát triển, là thành viên chiến lược của Tập đoàn tài chính Nhật Bản MUFG, hiện mở rộng sự hiện diện tại 5 quốc gia trong khu vực”

**1.1.2 Thành tựu, mục tiêu, tầm nhìn, sứ mệnh**

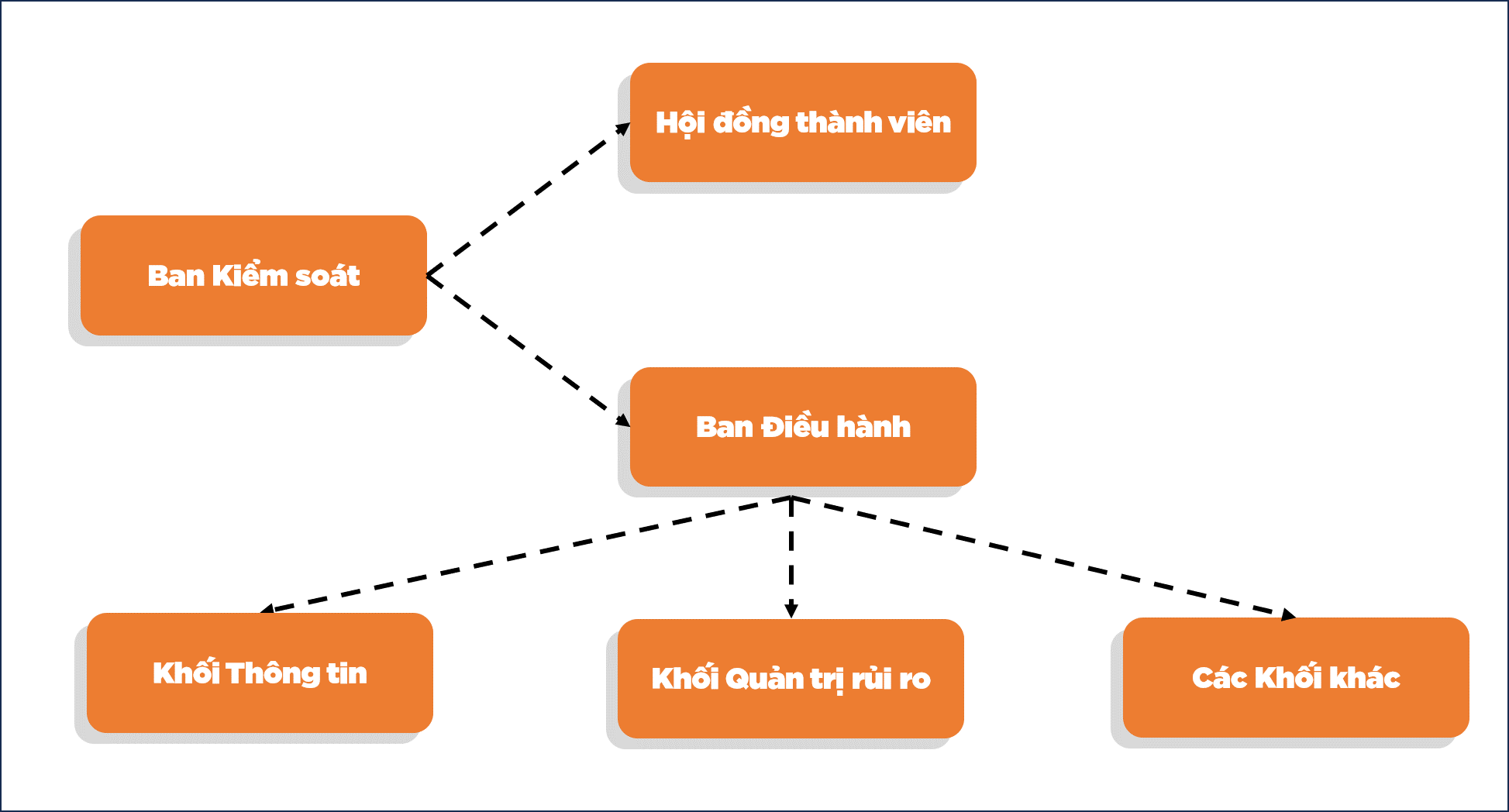
SHB Finance không chỉ có nhiều điểm nổi bật về việc cung cấp dịch vụ trong lĩnh vực hoạt động là Tài chính tiêu dùng, mà còn tạo công ăn việc làm cho gần 8000 người dân tại Việt Nam. Cụ thể là những ngành nghề như Bán hàng/Kinh doanh, Dịch vụ Ngân hàng và Tài chính cá nhân, Luật/Pháp lý, Ngân hàng, Quản trị rủi ro, Tài chính/Đầu tư. Với việc thấu hiểu rằng chăm sóc nhân viên tốt chính là cách để quảng bá sản phẩm tốt, SHB Finance cũng xây dựng chính sách đãi ngộ xứng đáng thông qua việc đào tạo, cung cấp bảo hiểm và cho vay vốn ưu đãi đối với CBNV. Thông qua việc điều hành hiệu quả, lấy khách hàng làm trung tâm, SHB Finance cũng đạt được một số thành tựu nhất định như:

* Top 6 Nhà tuyển dụng được yêu thích trong năm 2018
* Top 1 Nhà tuyển dụng được yêu thích nhất ngành nghề lĩnh vực Finance – Banking năm 2019
* Được Moody’s[[1]](#footnote-1) xếp hạng tín nhiệm lần đầu hạng Ba3 năm 2019
* Top 8 công ty tài chính tiêu dùng lớn nhất Việt Nam năm 2023
* Duy trì nợ xấu ở mức ổn định
* Phục vụ cho khoảng 300 nghìn hộ gia đình và 200 nghìn khách hàng

Cùng với đó là tầm nhìn “Trở thành Công ty Tài chính Thuận tiện và Tin cậy với người dân Việt Nam” và sứ mệnh “Cung cấp các giải pháp Tài chính tiêu dùng thông minh, dễ tiếp cận cho mọi người dân Việt”. Ngoài ra, SHB Finance cũng đưa ra bộ quy tắc ứng xử độc đáo, dựa trên năm chữ cái viết tắt “SHBFC” bao gồm: S – Smart, H – Honest, B – Brave, F – Friendly và C – Cooperative.

**1.1.3 Cơ cấu tổ chức**

Cơ cấu tổ chức của công ty Tài chính SHB Finance là cơ cấu của công ty TNHH từ hai thành viên trở lên. Bao gồm: Ban Kiểm soát sẽ giám sát, miễn/bổ nhiệm đối với Hội đồng thành viên và giám sát với Ban Điều hành. Hội đồng thành viên sẽ bầu chọn Ban Điều hành và Ban Điều hành sẽ trực tiếp quản lý các Khối.

****

Hình: Sơ đồ tổ chức của công ty Tài chính SHB Finance

**1.2 Mô tả bài toán**

**1.2.1 Thực trạng**

Trong hệ thống có số lượng giao dịch lớn, liên tục của các ngành, đặc biệt là ngành Tài chính – Ngân hàng, việc lựa chọn hệ quản trị cơ sở dữ liệu phù hợp là một phần quan trọng của việc xây dựng và duy trì ổn định các lô-gic, nghiệp vụ và nhận/trả yêu cầu của người dùng. Cơ sở luôn phải đảm bảo 4 đặc điểm – A (Atomicity, tính toàn vẹn), C (Consistency, tính nhất quán), I (Isolation, tính độc lập) và D (Durability, tính bền vững).

Oracle Database – hệ quản trị cơ sở dữ liệu quan hệ với bề dày lịch sử hơn 46 năm, hỗ trợ đa dạng nền tảng có thứ hạng đầu tính tới thời điểm tháng 9/2023 trên thị phần thế giới (*Most Popular Database Management Systems 2023 | Statista*, 2023). Với tính năng đa dạng, hiệu năng nổi trội và được chứng minh uy tín qua nhiều doanh nghiệp lớn, Công ty Tài chính tiêu dùng SHBFinance đã lựa chọn Oracle Database và sử dụng làm nền tảng cho các hệ thống tầng hỗ trợ nghiệp vụ, trong đó, có hệ thống Xếp hạng tín dụng nội bộ.

Trong SHB Finance, cũng như trong nhiều tổ chức tài chính khác, việc duy trì sự ổn định và liên tục của hệ thống thông tin là vô cùng quan trọng để đảm bảo hoạt động kinh doanh diễn ra một cách suôn sẻ. Hai chỉ số Mean Time Between Failure (MTBF) và Mean Time To Recovery (MTTR) là hai chỉ số quan trọng, phổ biến được dùng để đánh giá độ tin cậy của một hệ thống.

* **Mean Time Between Failure:** là chỉ số biểu thị thời gian trung bình giữa các lần lỗi/hỏng của một hệ thống. Đây là thước đo độ tin cậy và thường được sử dụng trong việc lập lịch bảo hành, kế hoạch bảo trì và phát triển sản phẩm. Được tính bằng *MTBF = Tổng thời gian vận hành / Tổng số lần hỏng trong một khoảng thời gian nhất định* (Stryker, 2023)
* **Mean Time To Recovery:** là chỉ số biểu thị thời gian trung bình để phục hồi một hệ thống sau khi gặp lỗi/hỏng. Mục tiêu của MTTR là giảm thiểu thời gian ngừng hoạt động do hỏng hóc liên quan đến việc sửa chữa. Được tính bằng *MTTR = Tổng thời gian ngừng hoạt động / Tổng số lần lỗi trong một thời gian cụ thể* (Stryker, 2023)

Để một hệ thống đạt được độ tin cậy cao, giảm thiệu rủi ro do gián đoạn, phải tiến tới việc điều chỉnh tăng chỉ số MTBF và giảm chỉ số MTTR. Hiện tại, với cơ sở dữ liệu Oracle mà SHBFinance sử dụng cho các hệ thống hỗ trợ, đang được sử dụng các giải pháp sao lưu như công cụ chính Recovery Manager (RMAN), sử dụng Oracle Flashback và Oracle Secure Backup (OSB) để tăng tính bảo mật cho bản sao lưu trong môi trường phân tán.

Với công cụ sao lưu chính RMAN, có thể sao lưu từ toàn bộ hệ thống cho đến một phần hệ thống ở cấp độ vật lý. Tuy nhiên, thời gian khôi phục của RMAN được chỉ rõ lên tới hàng giờ cho đến hàng ngày, chưa đáp ứng được việc giảm chỉ số MTTR. Thực tế, có một số bài báo nghiên cứu khoa học cũng chỉ ra một số điểm hạn chế của giải pháp này như:

* **Hạn chế về băng thông:** RMAN gặp hạn chế khi không thể sao lưu các tập dữ liệu lớn tới một hệ thống nằm ngoại mạng. Khi cần sao lưu, sẽ tiêu tốn rất nhiều tài nguyên mạng cũng như gặp vấn đề về thời gian, ảnh hưởng hiệu suất và các “thời điểm vàng” của SHBFinance
* **Hạn chế về thời gian khôi phục:** Trong trường hợp một thảm họa làm cho trung tâm dữ liệu bị lỗi, việc khôi phục dữ liệu từ các bản sao lưu RMAN gặp nhiều khó khăn. Nếu cả trung tâm dữ liệu và bản sao lưu đều bị mất, quá trình khôi phục dữ liệu sẽ gặp nhiều vấn đề và có thể tốn thời gian đáng kể (Yu et al.)

**1.2.2 Thách thức**

Khi hệ thống của một doanh nghiệp, đặc biệt là hoạt động về lĩnh vực Tài chính – Ngân hàng gặp vấn đề, như sụp đổ hoặc gián đoạn, không chỉ gây ảnh hưởng đến hoạt động kinh doanh hàng ngày mà còn mang theo nhiều thách thức lớn. Mất mát dữ liệu, không thể truy cập thông tin quan trọng để đưa ra quyết định kịp thời, và sự gián đoạn trong dịch vụ có thể dẫn đến mất lòng tin từ phía khách hàng, gây tổn thương về uy tín và doanh số của công ty. Hơn nữa, việc phục hồi hệ thống có thể đòi hỏi nhiều thời gian và chi phí, và không có kế hoạch hồi phục hiệu quả có thể làm gia tăng rủi ro và ảnh hưởng đến sức mạnh cạnh tranh của công ty trong ngành. Hơn hết, trong một môi trường kinh doanh đầy cạnh tranh như ngành tài chính, việc duy trì sự ổn định của hệ thống là một yếu tố quan trọng để bảo vệ uy tín và sự phát triển của doanh nghiệp.

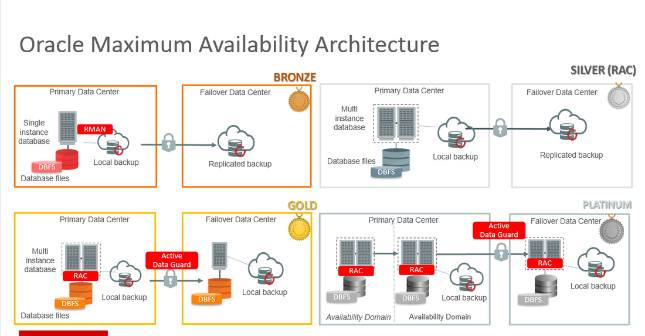
**1.2.3 Giá trị mang lại**

Để giải quyết thách thức về sao lưu và khôi phục dữ liệu tại SHBFinance, một quyết định cần được đưa ra với mục tiêu chính là đảm bảo rằng dữ liệu từ cơ sở dữ liệu luôn sẵn sàng cho hoạt động kinh doanh một cách nhanh chóng và đáng tin cậy. Điều này đòi hỏi một giải pháp hiệu quả có khả năng sao lưu và phục hồi dữ liệu tự động, giảm thiểu thời gian gián đoạn và mất mát dữ liệu. Một số giá trị lợi ích mà việc này mang lại có thể kể đến như:

* Khôi phục dữ liệu kịp thời: khôi phục dữ liệu nhanh chóng sau sự cố, giảm thiểu thời gian gián đoạn hoạt động kinh doanh và đảm bảo tính liên tục của các quy trình hoạt động.
* Tiến tới chuẩn Basel cao hơn trong lĩnh vực Tài chính – Ngân hàng: Bằng cách cung cấp khả năng khôi phục dữ liệu nhanh chóng và hiệu quả, giải pháp Data Guard giúp tổ chức tuân thủ các quy định và tiêu chuẩn của Basel liên quan đến quản lý rủi ro và bảo vệ dữ liệu, nâng cao uy tín và sự tin cậy của tổ chức trong mắt khách hàng và cơ quan giám sát.
* Tiết kiệm chi phí và thời gian: giảm thiểu chi phí và thời gian phục hồi sau sự cố, loại bỏ nhu cầu phải tiêu tốn nguồn lực nhân sự và vật lý để thực hiện các công việc sao lưu và khôi phục thủ công. Điều này giúp tổ chức tối ưu hóa hiệu suất và tài nguyên của họ, tập trung vào các hoạt động kinh doanh chính.

**1.2.4 Hướng giải quyết**

Để giải quyết bài toán đã nêu, cần thay đổi loại hình sao lưu – khôi phục mà SHBFinance đang sử dụng. Tham chiếu với khung giải pháp *Oracle Maximum Availability Architecture (MAA)* của Oracle, hiện trạng về phần trung tâm cơ sở dữ liệu dự phòng của hệ thống Xếp hạng tín dụng nội bộ của SHBFinance chỉ đạt ở mức Silver trở xuống. Với mức Gold trở lên, giải pháp Oracle Data Guard (ODG, Active Data Guard là tính năng, có từ phiên bản 11g) được giới thiệu rằng giúp quá trình vận hành của doanh nghiệp được đảm bảo liên tục, bằng cách giảm thiểu các sự cố không có chủ đích, gây ra thời gian dừng lâu hoặc các nghiệp vụ có chủ đích nhằm nâng cấp hệ thống thông qua việc chuyển đổi quá trình hoạt động, vận hành giữa CSDL chính (Primary) sang CSDL phụ (Standby). Vì vậy, đây chính là giải pháp thích hợp để triển khai cho hệ thống Xếp hạng tín dụng nội bộ của SHBFinance.



Hình: Khung tham chiếu giải pháp Oracle MAA

Giải pháp Oracle Data Guard có các đặc điểm như sau:

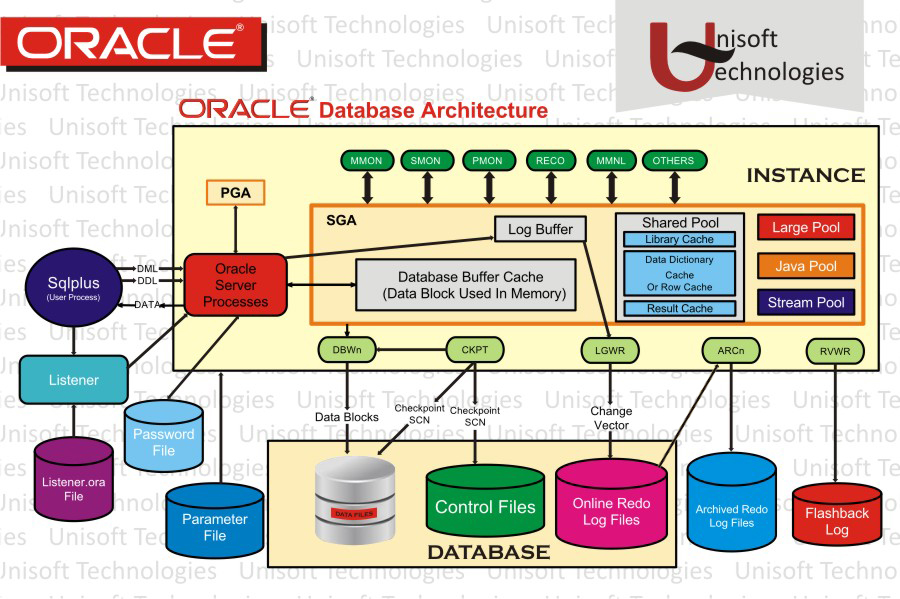
* Sao lưu dữ liệu theo thời gian thực: Oracle Data Guard cho phép sao lưu dữ liệu từ một cơ sở dữ liệu gốc (primary) sang một hoặc nhiều cơ sở dữ liệu dự phòng (standby) một cách đồng bộ và thời gian thực, đảm bảo rằng các bản sao luôn được cập nhật với dữ liệu mới nhất, đạt được tính toàn vẹn và tùy theo cấu hình hệ thống.
* Ứng biến kịp thời: Trong trường hợp sự cố xảy ra ở CSDL Primary, Oracle Data Guard tự động chuyển đổi sang một trong các CSDL Standby, giúp giảm thiểu thời gian chết hệ thống và tiếp tục phục vụ người dùng một cách liền mạch. Ngoài ra, ODG cho phép tạo dựng lên tới 30 CSDL Standby, giúp độ sẵn sàng của dữ liệu cao hơn.
* Phục vụ nhiều mục đích: Oracle Data Guard hỗ trợ nhiều loại CSDL ở chế độ dự phòng (gọi là standby), bao gồm physical standby, logical standby và snapshot standby, để phù hợp với nhu cầu cụ thể của doanh nghiệp và môi trường.
* Quản lý tự động: Oracle Data Guard cung cấp các công cụ quản lý tự động để giảm thiểu sự can thiệp của người quản trị, bao gồm cả việc tự động thực hiện các hoạt động như sao lưu, kiểm tra tính sẵn sàng và ghi nhật ký.
* Giảm tải cho hệ thống chính: kể từ phiên bản Oracle 11g trở đi, ODG cho phép các hệ thống máy người dùng truy vấn trực tiếp các dữ liệu được cập nhật theo thời gian ở chế độ chỉ đọc, và cũng cho phép sao lưu dữ liệu có trên CSDL Standby. Điều này giúp hệ thống CSDL Primary chỉ có nhiệm vụ vận hành, không cần phải tải thêm những nhiệm vụ phụ khác.

Nhờ một số tính năng liệt kê của Oracle Data Guard, đây là giải pháp nổi trội hơn các công cụ sao lưu nêu trước đang được dùng trong SHBFinance. Kết luận, đây là một giải pháp phù hợp với thực trạng cho cơ sở dữ liệu của hệ thống Xếp hạng tín dụng nội bộ của SHBFinacne.

**1.3 Giới thiệu về Oracle Data Guard**

**1.3.1 Kiến trúc Oracle Database**

Tổng quan, kiến trúc của hệ quản trị cơ sở dữ liệu Oracle gồm hai phần chính,Instance – giao tiếp trực tiếp với người dùng, là cầu nối cho người dùng tương tác với Database – bao gồm các tập tin vật lý, lưu trữ dưới ổ đĩa cứng, được cấu thành bởi File Systems (hệ thống tệp tin).



Hình: Kiến trúc tổng quan của Oracle Database

Trong Instance, chứa hai cấu trúc thành phần lớn:

* *Cấu trúc tiến trình (Process Structure)*: tập hợp các tiến trình thực hiện trong bộ nhớ RAM, là yếu tố quan trọng trong việc điều tiết dữ liệu từ các tệp tin vật lý đến bộ nhớ, cũng như cho việc sao lưu và phục hồi. Ngoài các tiến trình được nêu gọi là Background Processes, thì cũng có một số tiến trình khác như Server Processes, thực hiện các hoạt động liên quan đến phản hồi yêu cầu từ hệ thống máy người dùng cuối
* *Cấu trúc bộ nhớ (Memory Structure)*: vùng nhớ được hệ thống cấp phát khi khởi động Instance, bao gồm vùng nhớ dùng chung (System Global Area - SGA) và vùng nhớ dùng riêng (Program Global Area - PGA). Với vùng nhớ SGA, toàn bộ hoạt động liên quan tới hệ thống điều tiết luồng dữ liệu sẽ hoạt động tại đây. Vùng nhớ PGA được cấp phát riêng cho mỗi hệ thống máy người dùng cuối khi họ kết nối tới (nếu được thiết lập cấu hình Dedicated Server), chứa thông tin về thông tin kết nối tới cơ sở dữ liệu (CSDL), con trỏ trong việc dùng truy vấn và nhiều thông tin khác

Với Database, chưa cấu trúc thành phần *Cấu trúc lưu trữ (Storage Structure)*. Tập hợp các tập tin quan trọng để lưu trữ dữ liệu và khởi động CSDL. Các tập tin này có thể kể đến một số như sau:

* *Tập tin điều khiển (Control Files):* đây là tập tin quan trọng, chứa các thông tin về địa điểm của các tập tin dữ liệu và tập tin sao lưu. Ngoài ra, chúng cũng chứa thông tin meta-data về điểm khôi phục như System Change Number (SCN)
* *Tập tin dữ liệu (Data Files):* lưu trữ toàn bộ dữ liệu của CSDL do người dùng sinh ra, cũng như bao gồm cả những đối tượng của CSDL, người dùng phải thông qua Instance thì mới có thể đọc/ghi chính xác trên tập tin này
* *Tập tin lưu trữ thay đổi (Redo Log Files):* lưu trữ những thông tin thay đổi về dữ liệu, được gọi là những véc-tơ thay đổi (information vector changes). Bất kể là những thay đổi được ghi nhận (COMMIT) hay chưa ghi nhận (UNCOMMITTED) đểu được lưu trữ xuống đây, cùng với thông tin về SCN nhằm mục đích có thể khôi phục CSDL sau những trường hợp lỗi hệ thống (ROLLFORWARD)
* *Tập tin mật khẩu (Password File):* lưu trữ thông tin được mã hóa về mật khẩu của tài khoản người dùng quản trị hệ thống với các đặc quyền sâu về quản trị hệ thống như SYS, SYSTEM, SYSOPER
* *Tập tin cấu hình tham số (Parameters File):* lưu trữ thông tin về tham số khởi động, cấp phát bộ nhớ cho Instance. Thường tập tin này sẽ có hai dạng, văn bản thô đơn thuần (text – init.ora) và dạng nhị phân máy đọc (spfile.ora)

Để khởi động CSDL, cần vai trò của người quản trị thực hiện việc này, khi đăng nhập vào, hệ thống sẽ xác thực thông tin đăng nhập của người quản trị thông qua tệp tin mật khẩu. Khi khởi động CSDL với lệnh “startup” được yêu cầu từ SQL\*Plus hoặc bất kỳ công cụ nào dành cho người quản trị truy cập được vào môi trường hệ thống trạng thái IDLE Instance, CSDL sẽ khởi động theo các pha sau đây:

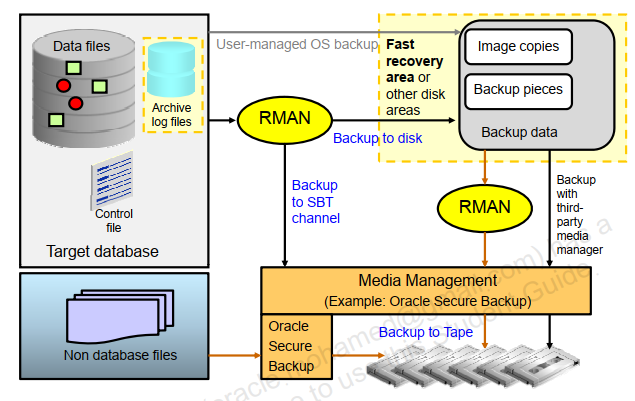
* Từ SHUTDOWN đến NOMOUNT: thực hiện tìm tệp tin cấu hình tham số và kích hoạt hệ thống cấp phát bộ nhớ SGA cho Instance, khởi động các Background Processes
* Từ NOMOUNT đến MOUNT: thực hiện tìm tệp tin điều khiển được xác định trong tệp tin cấu hình tham số. Từ đây, tệp tin điều khiển cung cấp cho hệ thống vị trí của các tệp tin dữ liệu cũng như các tệp tin lưu trữ thay đổi
* Từ NOMOUNT đến OPEN: tệp tin dữ liệu và tệp tin lưu trữ thay đổi sẵn sàng cho việc lưu trữ, hệ thống máy người dùng đã có thể kết nối tới và tương tác với CSDL. Các tiến trình Background Processes sẽ thực hiện kiểm tra tính đồng bộ giữa hai tệp tin và khôi phục nếu có lỗi

**1.3.2 Sao lưu với công cụ Recovery Manager (RMAN)**

Recovery Manager (RMAN) là một công cụ quản lý sao lưu và khôi phục dữ liệu tối ưu của Oracle, được thiết kế đặc biệt để hỗ trợ việc quản lý và bảo vệ dữ liệu trong các cơ sở dữ liệu Oracle. Mục đích cơ bản của RMAN là cung cấp các tính năng và công cụ cho việc thực hiện các tác vụ sao lưu và khôi phục dữ liệu một cách linh hoạt, hiệu quả và an toàn.

Đặc điểm nổi bật chính của RMAN là ngoài việc sao lưu khi CSDL đang tắt (Offline/Consistent/Cold), thì cũng có thể sao lưu ngay cả lúc CSDL đang hoạt động (Online/Inconsistent/Hot). Ngoài ra, RMAN cũng cung cấp tính năng sao lưu một phần, bao gồm chỉ những thay đổi kể từ bản sao lưu trước đó. Tương tự đối với việc khôi phục, công cụ cho phép khôi phục một phần hoặc toàn phần.

Các thành phần mà RMAN sao lưu bao gồm: Data Files, Control Files, Archived Redo Log, Parameters File. Đối với mức độ block – đơn vị nhỏ nhất trong kiến trúc lưu trữ vật lý, khi sao lưu, RMAN tự động kiểm tra những block rỗng và sẽ bỏ qua block này. Công cụ này cũng được tích hợp lên giao diện quản trị dành cho doanh nghiệp là Oracle Enterprise Manager và cũng có thể sử dụng bởi lệnh SQL để tạo. Ngoài ra, chúng cũng được tích hợp thêm thành phần Oracle Secure Backup để mã hóa và sao lưu ra ổ đĩa dạng băng từ (tape) hoặc sao lưu lên đám mây một cách bảo mật, an toàn.



Hình: Kết hợp RMAN, Oracle Secure Backup và sao lưu bằng lệnh hệ thống

**1.3.3 Khái niệm, kiến trúc và điểm chính của Oracle Data Guard**

**1.3.3.1 Khái niệm**

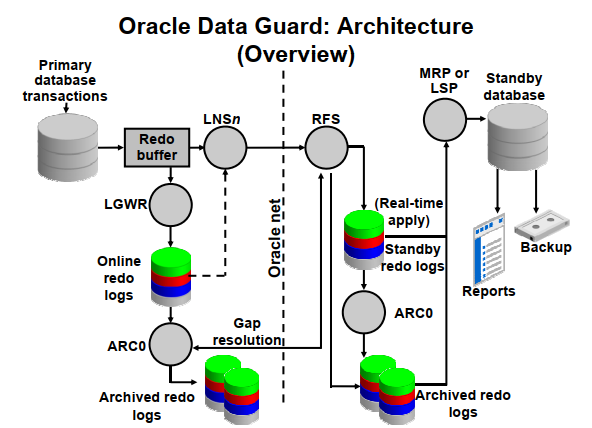
Giải pháp Oracle Data Guard được giới thiệu và triển khai kể từ phiên bản Oracle Database 7, kể từ đây, Oracle sử dụng thuật ngữ “Standby Database” để chỉ CSDL dự phòng. Tuy nhiên, phiên bản này có một hạn chế - các tệp tin ghi log được truyền tự động để sao lưu lại không thể lưu trữ (archive), nếu muốn, phải làm thao tác thủ công là viết mã hoặc lập trình để sao lưu. Kể từ phiên bản Oracle Database 8i, 9i, 9i R2 cho đến 10g thì các tính năng được cải thiện, đáp ứng nhu cầu gần như hoàn hảo của mọi doanh nghiệp, đó là không chỉ về truyền tải thời gian thực thông tin thay đổi và truy vấn trên CSDL Standby mà còn cho phép hành động ghi/đọc, sao lưu CSDL Standby và nhiều tính năng khác.

Trong các giải pháp phục hồi sau sự cố, Oracle Data Guard (ODG) là một công nghệ được đánh giá cao trong việc đảm bảo tính sẵn sàng và liên tục của CSDL Oracle. ODG được xây dựng và tích hợp trên CSDL Oracle, gồm nhiều mô-đun chức năng như quản lý, giám sát, tự động hóa quy trình, duy trì một hoặc nhiều CSDL Standby nhằm mục đích bảo vệ quy trình vận hành của doanh nghiệp khỏi sự cố, thảm họa, lỗi và các nghiệp vụ có chủ đích. CSDL Standby duy trì sự ổn định này bằng cách trở thành bản sao y của CSDL chính (Primary), phản ánh cùng một hiện trạng, trạng thái; CSDL Standby có thể đặt cách xa trung tâm dữ liệu của CSDL Primary để tăng thêm độ an toàn đề phòng trường hợp thiên tai ngay tại địa điểm đặt CSDL Primary. Khi CSDL Primary gặp sự cố, công nghệ ODG sẽ chuyển đổi sự vận hành (switch role) từ CSDL Primary – đang bị ảnh hưởng sang CSDL Standby, CSDL Standby sẽ đảm nhận vai trò thành CSDL Primary, từ đây giảm thiểu khỏi việc dữ liệu bị mất mát.

**1.3.3.2 Kiến trúc**

Trong kiến trúc của giải pháp ODG bao gồm 01 CSDL Primary và lên tới 30 CSDL Standby. Các hệ thống CSDL liên kết và giao tiếp với nhau thông qua một dịch vụ gọi là Oracle Network Service trong môi trường mạng của Oracle, các CSDL này có thể đặt cách xa nhau về mặt địa lý. Khoảng cách đặt hệ thống CSDL không phải là vấn đề, người triển khai giải pháp chỉ cần đảm bảo rằng các CSDL có thể giao tiếp với nhau thông qua môi trường mạng. Có nhiều cách triển khai CSDL dự phòng, có thể trong cùng một Server, xuất hiện đồng thời Primary và Standby, nhưng an toàn hơn thì cũng có thể có nhiều Server và mỗi CSDL thuộc về Server riêng.

CSDL Standby là bản sao y của CSDL Primary trong từng giao dịch (transactions). CSDL Standby được tạo dựng từ một bản sao lưu ban đầu của CSDL Primary. Ý tưởng của giải pháp ODG là tận dụng việc thông tin thay đổi được lưu dưới dạng véc-tơ có trong tệp tin lưu trữ thay đổi (redo log foles) để giữ cho CSDL Standby luôn được đồng bộ hóa nhờ việc chuyển và áp dụng những thay đổi đó của CSDL Primary.



Hình: Kiến trúc tổng quan giải pháp Oracle Data Guard

Trong kiến trúc giải pháp ODG sử dụng rất nhiều tiến trình phụ trợ, nhằm mục đích tự động hóa việc sao lưu và chuyển đổi vai trò. Có một số tiến trình thuộc về cấu trúc tiến trình chung của Oracle Database, và có một số tiến trình chỉ xuất hiện khi triển khai giải pháp ODG. Có thể liệt kê các thành phần và tiến trình khi phân loại theo Oracle Database so với giải pháp ODG như sau:

* Thành phần/Tiến trình chung trong Oracle Database
  + Redo Buffer: thành phần - bộ đệm lưu trữ thông tin véc-tơ thay đổi, các thông tin được gom nhóm và chuyển xuống Online Redo Logs theo từng đợt nhằm giảm thiểu việc I/O hệ thống
  + Online Redo Logs: thành phần - lưu trữ thông tin véc-tơ thay đổi trên đĩa, bao gồm cả COMMITED và UNCOMMITED TRANSACTION
  + Archived Redo Logs: thành phần – lưu trữ bản sao của Online Redo Logs mỗi khi có hiện tượng Log Switch xảy ra (khi một Online Redo Log Groups đã đầy các thông tin véc-tơ thay đổi, chuyển sang Groups khác)
  + Log Writer (LGWr): tiến trình – đưa các nhóm thông tin véc-tơ thay đổi từ Redo Buffer và ghi xuống Online Redo Logs ở đĩa
  + Archiver (ARCn): tiến trình – sao chép tệp tin lưu trữ thông tin thay đổi của Online Redo Log Groups khi xảy ra Log Switch
* Thành phần/Tiến trình riêng của giải pháp ODG
  + Standby Redo Logs: thành phần – bộ đệm lưu trữ thông tin véc-tơ thay đổi, nhưng là của CSDL Standby
  + Log Writer Network Server (LNSs): tiến trình – nhận thông tin véc-tơ thay đổi và chuyển cho CSDL Standby
  + Recmote File Server (RFS): tiến trình – nhận thông tin véc-tơ thay đổi từ LNSs
  + Managed Recovery Process/Logical Standby Process (MRP/LSP): tiến trình áp dụng các thay đổi từ Standby Redo Log vào dữ liệu trên CSDL Standby. Tiến trình MRP cho CSDL dạng Physical và LSP sử dụng cho CSDL dạng Logical

**1.3.4 Loại hình bảo vệ**

Giải pháp ODG cung cấp nhiều loại hình bảo vệ, mỗi loại hình có đặc điểm khác nhau, linh hoạt và phù hợp với nhu cầu hiện tại của doanh nghiệp. Có thể phân loại các loại hình theo hai góc độ: về loại hình CSDL Standby và về mức độ bảo vệ trong cơ chế truyền/đồng bộ hóa thông tin véc-tơ thay đổi giữa các CSDL.

**Phân loại theo loại hình CSDL Standby**:

* *CSDL Standby vật lý (Physical):*
  + Là sao y của CSDL Primary có cấu trúc File Systems và dữ liệu giống với CSDL Primary
  + Được đồng bộ hóa với CSDL Primary thông qua việc áp dụng dữ liệu thay đổi (redo data) từ CSDL Primary
  + Cho phép thực hiện đồng thời tác vụ trả kết quả truy vấn cũng như việc nhận và áp dụng dữ liệu thay đổi vào CSDL. Chỉ mở CSDL ở chế độ chỉ đọc (read only)
* *CSDL Standby lô-gic (Logical):*
  + Chỉ sao y với CSDL Primary ở mức độ lô-gic, bộ nhớ vật lý có thể sử dụng các tính năng khác như Oracle Automatic Storage Management (ASM) để quản lý tập tin khác với File Systems theo mặc định. Ngoài ra, cũng sẽ thiếu một số cấu trúc vật lý như index, view.
  + Được đồng bộ hóa với CSDL Primary thông qua việc nhận, chuyển hóa dữ liệu thay đổi thành SQL và thực thi trên CSDL Standby để áp dụng thay đổi. Điều này được thực hiện nhờ công cụ phân tích tệp tin ghi trữ logs là LogMiner
  + Cho phép thực hiện đồng thời các tác vụ trả kết quả truy vấn, áp dụng dữ liệu thay đổi vào CSDL, đặc biệt hơn là cho phép chỉnh sửa đối với các bảng, đối tượng không nằm trong vùng được áp dụng thay đổi. Mở CSDL ở chế độ đọc/ghi (Read/Write)
* *CSDL Standby Snapshot:*
  + Là loại sao y CSDL Primary, được chuyển từ CSDL Standby Physical sang
  + Cho phép thực hiện đọc/ghi trên toàn bộ cơ sở dữ liệu với mục đích kiểm thử
  + Sẽ không nhận và áp dụng các thông tin thay đổi
  + Các thay đổi sẽ bị ROLLBACK lại nếu như chuyển về CSDL Standby Physical

**Phân loại theo chế độ bảo vệ**

Khi đi đến phân loại theo chế độ bảo vệ, cấu hình của các chế độ phụ thuộc vào các đối số được cài đặt (cụ thể là trong tham số *LOG\_ARCHIVE\_DEST\_n*), có 04 đối số chính như sau:

* SYNC: Xác nhận các redo data được gửi sang CSDL Standby thành công trước khi giao dịch gây ra thay đổi được đánh dấu là COMMIT; nếu không, hệ thống sẽ dừng hoạt động/tiếp tục tùy thuộc vào chế độ bảo vệ được chọn
* ASYNC: Không xác nhận việc redo data được nhận bởi CSDL Standby, do đó, giao dịch có thể COMMIT ngay lập tức trên CSDL Primary
* AFFIRM: Xác nhận việc redo data nhận được *sau khi* được ghi vào Standby Redo Log của CSDL Standby bằng một tín hiệu Acknowledgement (ACK), tổng quan là gửi ACK sau khi cơ chế Input/Output (I/O) thành công
* NOAFFIRM: Khác với AFFIRM ở chỗ sẽ gửi tín hiệu ACK, nhưng *gửi trước* khi được ghi vào Standby Redo Logs

Về phân loại theo chế độ bảo vệ, bằng cách tinh chỉnh cách truyền thông tin thay đổi để hỗ trợ. Các chế độ này giúp doanh nghiệp cân bằng việc toàn vẹn dữ liệu và hiệu năng của hệ thống:

* *Ưu tiên bảo vệ (max. protection):* 
  + Chế độ bảo vệ mà CSDL Primary sẽ đảm bảo rằng không có dữ liệu nào bị sót một cách tuyệt đối trong trường hợp CSDL Primary gặp sự cố như thảm họa thiên tai, bị lỗi mạng hoặc bị lỗi với CSDL Standby
  + CSDL Primary sẽ dừng hoạt động khi gặp sự cố khiến cho các tiến trình trong việc truyền tải/đồng bộ hóa thông tin thay đổi không thể ghi vào ít nhất một trong các CSDL Standby
  + Thông tin thay đổi phải được xác nhận đã ghi vào tệp tin lưu trữ thông tin thay đổi ở cả CSDL Primary và ít nhất một CSDL Standby (gọi là Standby Redo Log) trước khi giao dịch được đánh dấu là COMMIT
  + Cần thiết lập hai chế độ cho cách truyền thông tin thay đổi với hai đối số: SYNC – đồng bộ hóa (tuần tự theo quá trình gửi redo data, Standby nhận redo data, gửi lại tín hiệu), cần tín hiệu acknowledgement (ACK) và AFFIRM – xác nhận đã ghi xuống đĩa vật lý tại Standby Redo Logs, với ít nhất một Standby có Standby Redo Logs
* *Ưu tiên tính sẵn sàng (max. availabilty):*
  + Chế độ bảo về mà CSDL Primary sẽ đảm bảo không có dữ liệu nào bị sót nhưng không hoàn toàn tuyệt đối, vì không tác động tới việc vận hành của CSDL Primary trong một ràng buộc về thời gian cho trước
  + Thông tin về thay đổi cũng phải được ghi vào Online Redo Log của Primary và Standby (Standby Redo Log) và truyền thông qua các tiến trình LNSs và RFS
  + Tuy nhiên, CSDL Primary sẽ không dừng hoạt động nếu có sự cố không thể xác nhận CSDL Standby đã ghi/nhận hay chưa
  + Nếu có sự cố, CSDL Primary sẽ hoạt động theo cách thức bất động bộ (ASYNC, hoạt động không đợi xác nhận Standby đã nhận redo data hay chưa) cho đến khi ít nhất một CSDL Standby được đồng bộ về mặt thông tin thay đổi, xử lý các khoảng trống giữa dữ liệu bằng tiến trình Fetch Archived Log (FAL). Hiểu đơn giản, hệ thống sẽ chuyển sang chế độ *max. performance* để hoạt động
  + Cần thiết lập hai đối số: SYNC – đồng bộ hóa (tuần tự) và NOAFFIRM (không cần xác nhận đã ghi vào Standby Redo Logs) hoặc AFFIRM cho ít nhất một CSDL Standby có chứa Standby Redo Logs
* *Ưu tiên hiệu năng hệ thống (max. performance):*
  + Đây là chế độ mặc định của giải pháp ODG. Cung cấp việc bảo vệ dữ liệu thấp hơn hai mức còn lại về tính vẹn toàn, kịp thời nhưng hiệu năng hệ thống được tăng trên CSDL Primary
  + Giao dịch được xác nhận COMMIT, đồng thời thông tin thay đổi sẽ được lưu xuống tệp tin lưu trữ thông tin thay đổi ngay lập tức mà không cần quá trình xác nhận (ACK - acknowledgement) từ CSDL Standby
  + Thông tin thay đổi (redo data) được truyền tới CSDL Standby theo cách bất đồng bộ (ASYNC, các quá trình không phải đợi nhau lần lượt) với những thông tin thay đổi đã được COMMIT
  + Cần cấu hình đối số như sau: ASYNC – bất đồng bộ và NOAFFIRM – không xác nhận đã ghi cho CSDL Standby đã có Standby Redo Logs
  + Điều đặc biệt là khi băng thông mạng lớn, chế độ ưu tiên hiệu năng cung cấp việc truyền tải thông tin thay đổi gần tương tự với chế độ ưu tiên tính sẵn sàng mà vẫn đảm bảo hiệu năng cao

Bảng so sánh về các chế độ bảo vệ dưới đây sẽ có cái nhìn tổng quan và ngắn gọn hơn. Lưu ý rằng, đây là các kết hợp đối số có ý nghĩa, có một số trường hợp kết hợp đối số khác không được chấp nhận như ASYNC/AFFIRM:

|  |  |  |  |
| --- | --- | --- | --- |
| **Chế độ** | **Rủi ro** | **Chế độ truyền** | **Nếu tín hiệu ACK không gửi (AFFIRM/NOAFFIRM)** |
| Ưu tiên bảo vệ | Không mất đồng bộ dữ liệu và không mất dữ liệu, đảm bảo tính toàn vẹn ở cả hai CSDL | SYNC | CSDL Primary sẽ treo/dừng hoạt động cho đến khi nhận được tín hiệu ACK |
| Ưu tiên tính sẵn sàng | Không mất đồng bộ dữ liệu, đảm bảo tính sẵn sàng của CSDL chính và có thể đảm bảo toàn phần dữ liệu | SYNC/AFFIRM | CSDL Primary sẽ chờ trong một khoảng thời gian được xác định là Time-to-Live, nếu hết, sẽ tiếp tục hoạt động, xử lý phần thiếu với tiến trình FAL |
| Ưu tiên tính sẵn sàng | Rủi ro trong việc mất dữ liệu nếu các CSDL đều lỗi | SYNC/NOAFFIRM (Tính năng Fast-Sync) | CSDL Primary sẽ chờ trong một khoảng thời gian được xác định là Time-to-Live, nếu hết, sẽ tiếp tục hoạt động, xử lý phần thiếu với tiến trình FAL |
| Ưu tiên hiệu năng | Rủi ro trong việc mất đồng bộ dữ liệu cao nếu gặp vấn đề truyền và CSDL Primary lỗi | ASYNC | CSDL Primary không chờ tín hiệu ACK |

Bảng: Cấu hình đối số phương thức truyền/xác nhận

**Cấu hình bảo vệ nâng cao với Far Sync**

Tính năng Far Sync là một hệ thống CSDL Standby cho phép là điểm trung chuyển thông tin thay đổi tới nhiều các Standby khác nếu hệ thống mạng lưới có nhiều CSDL Standby. Thực tế, Far Sync Standby là một hệ thống có kích thước gọn nhẹ, tiêu thụ ít tài nguyên về lưu trữ cũng như xử lý.

Far Sync Standby giống với CSDL Standby thông thường ở điểm quản lý các Control File, nhận redo data vào Standby Redo Logs và lưu trữ khi Log Switch xuống Archived Redo Logs. Ngược lại, khác với CSDL Standby ở điểm không lưu trữ một số tệp tin không quan trọng như Data Files, không hỗ trợ chuyển đổi vai trò và chỉ thiết lập được tại 02 chế độ bảo vệ: *max. performance* hoặc *max. availability*.



Hình: Tính năng Far Sync trong giải pháp Oracle Data Guard

Có thể kể đến một số lợi ích mà tính năng Far Sync đem lại như:

* Trong chế độ *max. availability* (SYNC/AFFIRM hoặc SYNC/NOAFFIRM – FastSync), Far Sync Standby hoạt động gần giống như CSDL Primary bằng việc giảm độ trễ trong việc phản hồi tín hiệu ACK khi đồng bộ hóa bản sao (đối với CSDL Primary, khi là trung gian chuyển đến các Standby khác). Nếu CSDL Primary lỗi, các CSDL Standby sẽ lấy các redo data cuối cùng từ Far Sync Standby trong việc chuyển đổi vai trò, đảm bảo tính vẹn toàn
* Trong chế độ *max. performance* (ASYNC/NOAFFIRM), Far Sync Standby không bị đặt nặng vấn đề khoảng cách do cách truyền bất đồng bộ, không ảnh hưởng đến hiệu năng của CSDL Primary. Hơn hết, Far Sync Standby giúp giảm tải CSDL Primary rất nhiều trong việc truyền tải redo data đến hàng loại CSDL Standby
* Ngoài ra, việc bổ sung các tính năng như đóng gói, mã hóa dữ liệu được Far Sync Standby đảm nhận nhằm giảm tải cho CSDL chính

**1.3.5 Cơ chế tương tác giữa các thành phần**

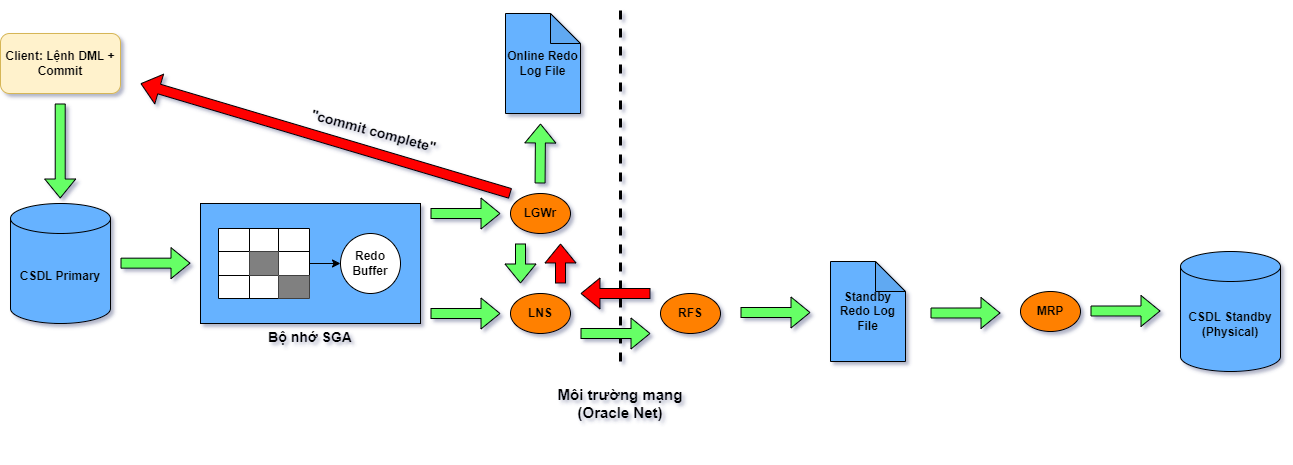
Các thành phần giao tiếp với nhau trong kiến trúc giải pháp Oracle Data Guard thông qua 03 cơ chế chính:

* Cơ chế vận chuyển thông tin thay đổi (Redo Transport Services): tự động hóa việc kiểm soát, điều khiển thông tin thay đổi từ CSDL Primary sang CSDL Standby
* Cơ chế áp dụng thông tin thay đổi (Redo Apply Services): tự động hóa việc áp dụng thông tin và cách áp dụng thay đổi khi nhận được thông tin thay đổi. Với CSDL Standby Physical, thông tin thay đổi được áp dụng thông qua việc khôi phục với công nghệ Oracle Media Recovery (được sử dụng trong RMAN). Với CSDL Standby Logical, thông tin thay đổi được LogMiner phiên dịch thành SQL và thực thi SQL để áp dụng thay đổi.
* Cơ chế quản lý/chuyển đổi vai trò (Role Management Services): là một tiến trình nền (Background Process), thực hiện thay đổi vai trò của Standby sang Primary khi CSDL Primary gặp lỗi, hệ thống dừng hoạt động. Trong đó, Switchover – thay đổi có kế hoạch và Failover – thay đổi khi gặp sự cố không lường trước được.

Cơ chế hoạt động của Oracle Data Guard thể hiện rõ nhất ở việc lựa chọn chế độ bảo vệ. Hai chế độ bảo vệ *Ưu tiên hiệu năng* và *Ưu tiên bảo vệ* có những đặc điểm nổi trội khác nhau, đặc biệt hơn so với *Ưu tiên về tính sẵn sàng*. Vì vậy, để hiểu được rõ được sự khác biệt và cơ chế hoạt động của luồng dữ liệu, hình vẽ cùng miêu tả các pha sẽ minh họa cơ chế hoạt động hai chế độ, hoạt động trong loại CSDL Standby vật lý (với tiến trình áp dụng thay đổi là MRP).

Với các hình vẽ minh họa, màu vàng be thể hiện hoạt động từ phía hệ thống máy người dùng, màu xanh thể hiện các thành phần chung hoặc CSDL, màu cam thể hiện tiến trình, màu xanh và đỏ thể hiện luồng đi thông tin.

**Chế độ bảo vệ *Ưu tiên bảo vệ***

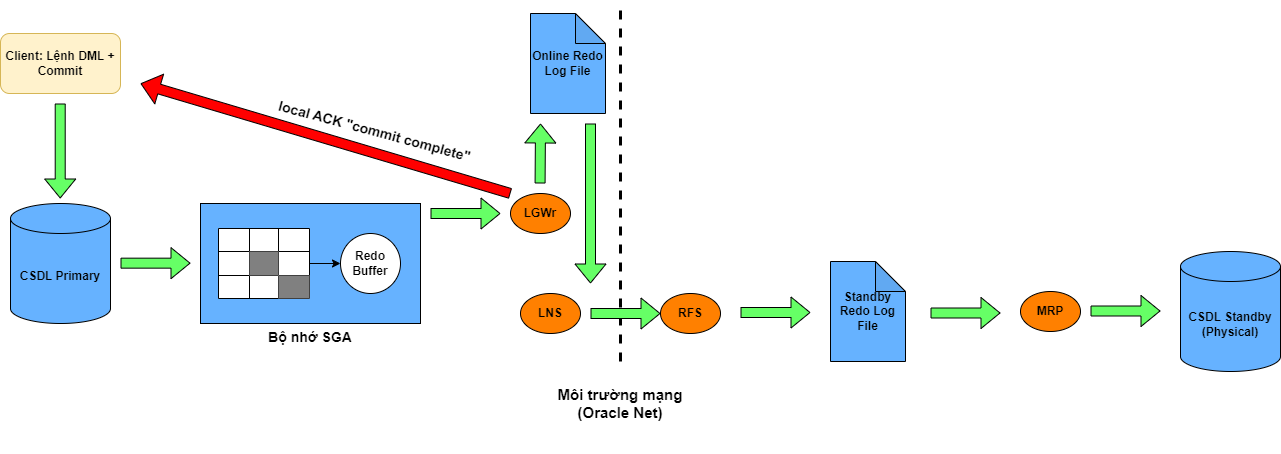


Hình: Minh họa luồng hoạt động của Oracle Data Guard với chế độ *Ưu tiên bảo vệ*

Các pha của cơ chế *Ưu tiên bảo vệ* được thể hiện tuần tự với các bước như sau, khi cấu hình SYNC/AFFIRM:

1. Người dùng sử dụng ứng dụng để giao tiếp với CSDL Primary. Người dùng ra lệnh dạng Data Manipulation Language (DML) như INSERT, UPDATE, DELETE và yêu cầu COMMIT. Vì với cấu hình SYNC/AFFIRM cho chế độ ưu tiên bảo vệ, cho nên, hệ thống chưa xác nhận COMMIT ngay lúc này do chưa nhận được xác nhận từ bên CSDL Standby đã áp dụng thay đổi vào đĩa
2. Trong CSDL Primary, tiến trình Server Process sẽ lấy dữ liệu cần thay đổi theo đơn vị block từ đĩa cứng lên Data Buffer Cache. Tại đây, các dữ liệu gốc (một block có thể là một dòng hoặc rất nhiều dòng dữ liệu) sẽ được thay đổi theo yêu cầu của lệnh DML. Block sau khi chỉnh sửa sẽ được đánh dấu là “dirty block”, ngoài ra, Redo Buffer Cache sẽ lưu lại các thông tin về thay đổi của dirty block theo dạng véc-tơ (gọi là redo data), có thể minh họa dễ hiểu như “Dòng ID xxx UPDATE từ zzz sang yyy, số SCN 1234, …”
3. Thông tin thay đổi sẽ được tiến trình LGWR đưa và lưu xuống Online Redo Log do có tín hiệu COMMIT, nhưng khi đã lưu, hệ thống chưa báo “commit complete” ngay. Lưu ý: lúc này, dữ liệu được thay đổi trên Data Buffer Cache chưa được lưu xuống đĩa, chỉ lưu khi xảy ra sự kiện Checkpoint thực hiện hoặc nguyên nhân khác
4. Tiến trình LNS sẽ nhận những thông tin thay đổi trong lúc LGWR xuất ra. Những thông tin thay đổi này sẽ được chuyển cho tiến trình RFS thuộc CSDL Standby, nhằm thực hiện sao lưu
5. Sau khi nhận được thông tin thay đổi, tiến trình RFS sẽ ghi những thông tin thay đổi xuống Standby Redo Log Files
6. Nếu CSDL Standby sử dụng tính năng Real-time Apply, thì ngay lập tức, các thông tin thay đổi này sẽ được áp dụng vào dữ liệu lưu trữ vật lý tại CSDL Standby với tiến trình khôi phục Media Recovery Process (MRP) dành cho loại Physical Standby
7. Với SYNC/AFFIRM, sau khi dữ liệu đã được áp dụng thành công, tiến trình RFS sẽ phản hồi lại cho tiến trình LNS thông tin (gọi là tín hiệu acknowledgement - ACK), lúc này, hệ thống mới tiến đến phản hồi người dùng “commit complete”. Tại đây, nếu gặp sự cố về môi trường mạng, khiến cho RFS không thể gửi cho LNS, CSDL Primary sẽ đợi tới khi nào nhận được thông tin dẫn tới hệ thống treo
8. LNS chuyển tiếp cho LGWR để hệ thống phản hồi lại cho người dùng thông báo COMMIT thực hiện thành công. Kết thúc quá trình của lệnh DML và COMMIT

**Chế độ *Ưu tiên hiệu năng***



Hình: Minh họa luồng hoạt động của Oracle Data Guard với chế độ *Ưu tiên bảo vệ*

Nhìn chung, trong chế độ ưu tiên hiệu năng, luồng dữ liệu không thay đổi nhiều. Tuy nhiên, với cơ chế ASYNC/NOAFFIRM, tức là hệ thống CSDL Primary sẽ không yêu cầu nhận bất kỳ tín hiệu xác nhận nào từ CSDL Standby trong việc ghi/áp dụng thay đổi thành công.

Khi người dùng gõ lệnh DML và yêu cầu COMMIT, hệ thống sẽ ngay lập tức trả lại tín hiệu COMMIT thành công – “commit complete”, do không phải chờ phản hồi từ CSDL Standby. Ở đây, tín hiệu ACK còn được gọi là “local ACK”, có nghĩa là tín hiệu này sẽ không xuất phát từ tiến trình RFS truyền qua môi trường mà CSDL Standby chứa đựng. Như vậy, hiệu năng hệ thống sẽ tăng lên đáng kể, nhưng rủi ro trong việc đảm bảo dữ liệu đồng bộ hóa và trong tính toàn vẹn là rất lớn.

Ngoài ra, để tăng hiệu năng hệ thống trong việc I/O tại đĩa, tiến trình LGWR cũng sẽ không chia sẻ thông tin thay đổi, mà LNS sẽ tự trích xuất từ Online Redo Logs và chuyển tiếp cho CSDL Standby.

**Cơ chế Log Delay và tính năng Gap Detection**

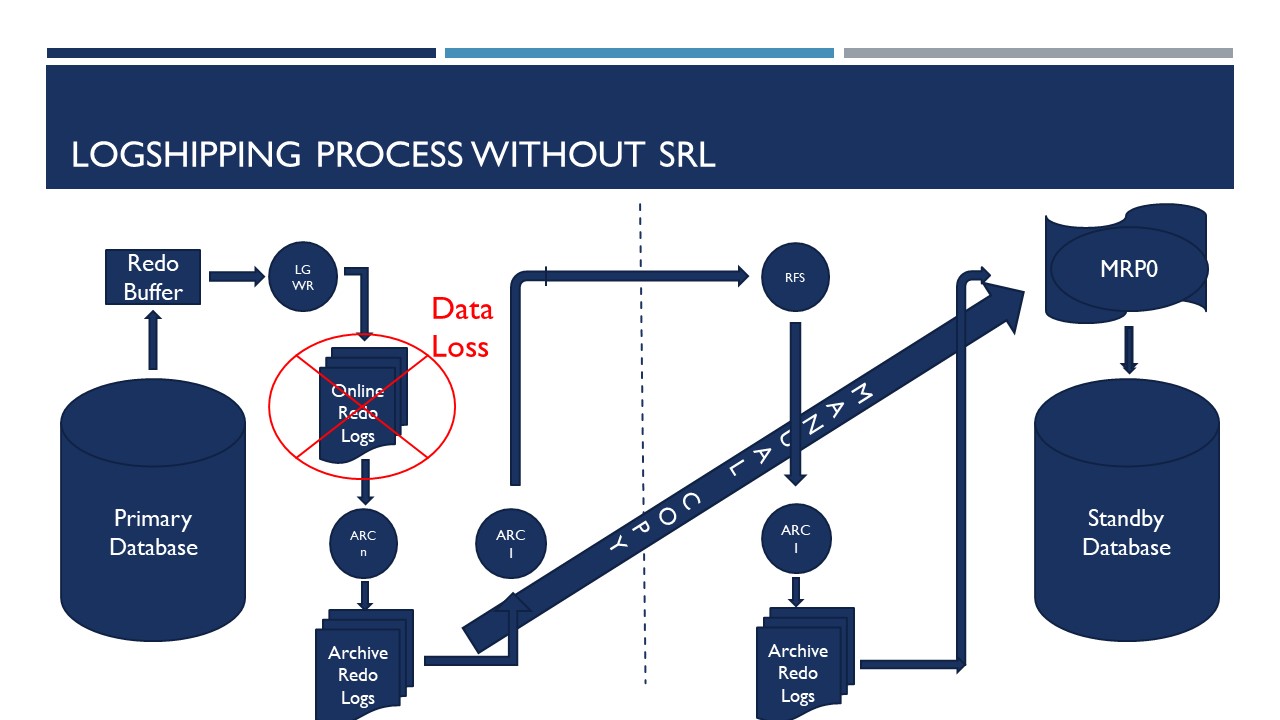
Trong kiến trúc của Oracle Data Guard cũng thể hiện thêm những đường kết nối khác, thể hiện cho cấu hình tham số khác, tùy chỉnh theo yêu cầu của tổ chức, doanh nghiệp. Như cấu hình tham số liên quan tới ghi thay đổi nhưng tăng độ trễ, vì có thể liên quan tới vấn đề đường truyền, hiệu năng hạn chế. Lúc này, redo data thay vì từ Standby Redo Log File áp dụng trực tiếp tới CSDL Standby, sẽ lưu xuống Archived Log File rồi mới áp dụng thay đổi. Tham số này gọi là Log Delay.

Ngoài ra, cũng có thêm vấn đề về tính khác biệt, khoảng cách về tính cập nhật của dữ liệu bị chậm khi hệ thống vừa mới đồng bộ hóa lại sau khoảng thời gian mất tín hiệu mạng. Lúc này, tính năng xử lý độ trễ dữ liệu (gọi là Gap Detection) sẽ hoạt động như sau: tiến trình RFS của Standby thực hiện trích xuất dữ liệu từ Archived Log File của CSDL Primary, đứng giữa là tiến trình Fetch Archived Log (FAL) hỗ trợ, RFS sẽ lưu vào Archived Log File của CSDL Standby nhằm khắc phục những phần thiếu do sự cố gây ra.

**Tầm quan trọng của Standby Redo Log Files trong cơ chế hoạt động**

Trước khi xuất hiện Standby Redo Log Files được giới thiệu tại phiên bản Oracle 9i, thì tiến trình RFS sẽ đọc trực tiếp thông tin thay đổi trong Archived Redo Log Files của CSDL Primary với sự trợ giúp trích xuất của tiến trình ACRn và ghi thông tin này vào Archived Redo Logs của CSDL Standby. Sau đó, thông tin thay đổi này mới được sử dụng thông qua quá trình khôi phục CSDL với tiến trình MRP để thực hiện áp dụng thay đổi vào CSDL Standby.

Hạn chế của kiến trúc này là do chỉ có một luồng dữ liệu duy nhất đi từ CSDL Primary, thông tin thay đổi từ Online Redo Logs phải ghi xuống Archived Redo Logs rồi mới được vận chuyển qua CSDL Standby. Một khi CSDL Primary gặp sự cố, tiến hành chuyển đổi vai trò fail-over, những thông tin thay đổi trong Online Redo Logs chưa được lưu xuống Archived Redo Logs (VD: Log Switch chưa xảy ra), gây ra hiện tượng lệch dữ liệu, khiến việc vận hành hệ thống không được nhất quán, sai kết quả trong luồng nghiệp vụ. Ngoài ra, việc cập nhật dữ liệu sang CSDL Standby cũng sẽ không được giống kịp thời với CSDL Primary, do thông tin thay đổi lấy được là những thông tin thay đổi được lưu xuống, tuần tự chuyển sang CSDL Standby sau một khoảng thời gian lưu vào Online Redo Logs cho tới khi cơ chế Log Switch xảy ra.



Hình: Kiến trúc của Oracle Data Guard trước khi giới thiệu Standby Redo Log Files

Sau khi Oracle bổ sung thêm Standby Redo Log Files, kiến trúc Oracle Data Guard hoạt động với việc vận chuyển thông tin thay đổi từ Online Redo Logs sang Standby Redo Logs, từ đây, hệ thống CSDL Standby có thể áp dụng thông tin thay đổi với phương thức “real-time apply” một cách nhanh chóng, kịp thời, đảm bảo tính vẹn toàn và đồng bộ. Khi này, cũng xuất hiện tiến trình LNS để phụ trợ và giảm tải tiến trình LGWR việc nhận và truyền redo data. LNS là tên gọi chung của hai tiến trình con Network Server Async (NSA) – dùng trong chế độ ASYNC/NOAFFIRM và Network Server Sync (NSS) – dùng trong chế độ SYNC/AFFIRM.

Standby Redo Log File có nhiệm vụ giống với Online Redo Log, lưu trữ dưới đĩa những thông tin thay đổi tạm thời (nếu có Archived Log Files, sẽ lưu lâu hơn) và xoay vòng khi các nhóm Standby Redo Log File hết không gian lưu trữ. Thuật ngữ Standby Redo Log dùng để chỉ thành phần riêng biệt để lưu trữ redo data được nhận từ CSDL khác.

Standby Redo Logs đóng vai trò quan trọng trong chế độ *Ưu tiên bảo vệ* hoặc *Ưu tiên tính sẵn sàng* bằng việc làm giảm thời gian để hệ thống xác nhận một giao dịch đã được ghi lại thay đổi ở cả hai loại CSDL Primary và CSDL Standby sau khi COMMIT. Điều này được thể hiện ở chỗ, tính năng Real-Time Apply chỉ hỗ trợ Standby Redo Logs, các thông tin thay đổi sau khi được chuyển tới Standby Redo Logs bằng tiến trình RFS, sẽ được áp dụng ngay vào CSDL Standby, thay vì phải chờ Log Switch xuất hiện ở CSDL Primary, chuyển xuống Archived Redo Log rồi mới được chuyển sang CSDL Standby. Standby Redo Logs cũng góp phần giảm việc mất mát dữ liệu, giữ trạng thái CSDL Standby luôn “near real-time” trong chế độ *Ưu tiên hiệu năng*, cũng bởi thông tin thay đổi được gửi trực tiếp tới Standby Redo Log.

Trong tổ chức/doanh nghiệp, lượng dữ liệu rất lớn, dẫn tới kéo theo cấu hình Online Redo Logs lớn, vì vậy, Log Switch xảy ra có thể từ hàng chục phút cho tới hàng tiếng; nếu không có Standby Redo Logs để có thể lưu trữ trực tiếp thông tin thay đổi mà CSDL Primary gặp sự cố, tổ chức/doanh nghiệp cũng sẽ mất một lượng dữ liệu khổng lồ khi fail-over sang CSDL Standby. Vì vậy, vai trò của việc thiết lập Standby Redo Logs là cực kỳ quan trọng, đảm bảo tính toàn vẹn và tối ưu trong việc vận hành.

**1.3.6 Sự khác biệt với các giải pháp sao lưu khôi phục khác (Advanced Replication, OS-level Replication, Storage-level Replication, RMAN backup, Disaster Recovery by Standby Redo Log)**

**1.3.7 Kết luận chương I**

1. Moody's là một cơ quan đánh giá tín nhiệm tín dụng hàng đầu trên thế giới. Họ cung cấp các báo cáo và xếp hạng tín dụng cho các công ty, quốc gia và các tổ chức khác để đánh giá khả năng trả nợ của họ và độ rủi ro đầu tư. [↑](#footnote-ref-1)