[I. Tổng quan bảo mật oracle 2](#_Toc515740279)

[I.1. Giới thiệu 2](#_Toc515740280)

[I.2. Nhận định chung 2](#_Toc515740281)

[I.3. Nguy cơ tiềm ẩn 3](#_Toc515740282)

[I.4. Thách thức 4](#_Toc515740283)

[II. Một số giải pháp bảo mật Oracle 4](#_Toc515740284)

1. Các tính năng bảo mật mặc định của Oracle

[2. Giới thiệu kiến trúc bảo mật Oracle Defense In Dept 4](#_Toc515740285)

[2.1. Giải pháp bảo mật Oracle Database Defense in Dept: 5](#_Toc515740286)

[2.2. Giải pháp Advanced Security 7](#_Toc515740287)

[2.3. Giải pháp bảo mật Oracle Data Masking 8](#_Toc515740288)

[2.4. Giải pháp bảo mật Oracle Secure Backup 8](#_Toc515740289)

[2.5. Giải pháp bảo mật Oracle Database Vault 9](#_Toc515740290)

[2.6. Giải pháp bảo mật Oracle Audit Vault 10](#_Toc515740291)

[2.7. Giải pháp bảo mật Oracle Label Security 11](#_Toc515740292)

[2.8. Giải pháp bảo mật Oracle Total Recall 12](#_Toc515740293)

[2.9. Giải pháp bảo mật Oracle Configuration Management 13](#_Toc515740294)

[3. Giải pháp Bảo mật CSDL riêng ảo trên Oracle 14](#_Toc515740295)

[4. Giải pháp bảo mật dựa vào nhãn trên Oracle 15](#_Toc515740296)

[III. Kết luận 17](#_Toc515740297)

**Bảo mật Oracle**

1. **Tổng quan bảo mật oracle**

## I.1. Giới thiệu

Oracle Database là thành phần rất quan trọng của tổ chức, doanh nghiệp. Bên cạnh việc lưu giữ thông tin về khách hàng, tài nguyên, con người, Database còn góp phần quan trọng trong việc phân tích và định hướng các chính sách phát triển của doanh nghiệp. Vì vậy, một điều tối quan trọng của doanh nghiệp là phải bảo mật Oracle Database trước những rủi ro, xâm nhập, mất thông tin. Tuy nhiên, thách thức đặt ra cho doanh nghiệp làm sao để “bảo mật dữ liệu an toàn” trước những rủi ro xâm phạm dữ liệu có thể xảy ra?

Oracle là một hệ quản trị CSDL được thiết kế nhằm triển khai cho môi trường doanh nghiệp. Nó cung cấp nhiều tính năng bảo mật nổi trội như: Giải pháp bảo mật Oracle Defense in Dept, an toàn dựa vào nhãn (Oracle Label Security - OLS), CSDL riêng ảo (Virtual Private Database - VPD), mã hóa dữ liệu trong suốt (Transparent Data Encryption - TDE), các cơ chế xác thực mạnh, các cơ chế sao lưu/dự phòng an toàn,.… WECOMMIT xin giới thiệu với các anh chị giải pháp bảo mật Oracle toàn diện, giải pháp hợp nhất bảo mật toàn diện hệ thống Oracle Database của doanh nghiệp.

## I.2. Nhận định chung

Hiện nay đa số các doanh nghiệp đều trang bị các giải pháp bảo mật Oracle như hệ thống tường lửa, hệ thống phát hiện xâm nhập, các kỹ thuật chóng spam nhằm đảm bảo hệ thống an toàn và hoạt động thông suốt trước các cuộc tấn công và xâm nhập từ bên ngoài với mục đích xâu. Tuy nhiên hệ thống bảo mật Oracle vẫn còn có những rủi ro, nguy cơ từ bên trong là không thể kiểm soát được. Do đó, vấn đề đặt ra là làm sao để đảm bảo an toàn dữ liệu trước các nguy cơ tấn công từ bên ngoài và các rủi ro từ bên trong là cần thiết.

Giải pháp được yêu cầu đưa ra để đảm bảo an toàn bảo mật dữ liệu là phải bảo vệ  CSDL theo chiều sâu, cho phép kiểm soát các hoạt động mang tính ngăn chặn và theo dõi bằng cách thực hiện các chính sách bảo mật “cần biết - need-to-know” và “ tin tưởng nhưng xác thực - trust-but-verify”

## I.3. Nguy cơ tiềm ẩn

Theo khảo sát cho thấy vấn đề bảo mật dữ liệu Oracle hiện nay của các Doanh Nghiêp vẫn chưa được quan tâm nhiều. Mặc dù các doanh nghiệp hiện nay đều đã trang bị các hệ thống bảo mật tiên tiến và tốn kém. Tuy vậy, các hệ thống Database vẫn còn chưa được bảo mật một cách triệt để. Một lý do đơn giản để giải thích cho vấn đề này, các hệ thống tuy được bảo mật, nhưng chỉ được bảo vệ bên ngoài. Các chính sách bảo vệ các rủi ro từ bên trong vẫn chưa được xem xét và đầu tư hợp lý và theo chiều sâu.

Theo một cuộc khảo sát an ninh bảo mật Database từ tổ chứ OIUG (Independent Oracle User Group) cho thấy:

* Đa số doanh nghiệp ngày nay không mã hóa dữ liệu trên đường truyền, các tập tin sao lưu.
* Việc thử nghiệm dữ liệu được thực hiện trên môi trường dữ liệu thật, không phải dữ liệu dành cho môi trường thử nghiệm.
* Cứ năm chuyên gia về dữ liệu khi được hỏi về bảo mật hệ thống dữ liệu trước các lỗ hổng bảo mật và các cuộc tấn công thì chỉ có một người khẳng định hệ thống được đảm bảo trước các cuộc tấn công
* Hiện nay, gửi dữ liệu ra bên ngoài đã trở nên phổ biến hơn
* Các hệ thống database vẫn chưa được cấu hình theo dõi hoặc bảo mật
* Người dùng được cấp một số quyền không cần thiết, leo thang thành các quyền cao hơn, có thể truy xuất vào dữ liệu quan trọng.
* Các lỗ hỏng về bảo mật không được cập nhật và theo dõi thường xuyên
* Đa số các doanh nghiệp đều nhận thấy các rủi ro lớn nhất từ việc truy cập bên trong, hoặc bởi những tài khoản không xác thực và những tài khoản có quyền tối cao như SYSDBA
* Hầu hết các doanh nghiệp đều không có chính sách ngăn cản người quản trị tối cao truy cập vào những dữ liệu quan trọng, chiến lược.

## I.4. Thách thức

Hiệ nay thách thức bảo mật an toàn thông tin, tránh việc mất mác dữ liệu là điều tối quan trọng đối với doanh nghiệp cũng như các tổ chức. Tuy nhiên vấn đề đặt ra khi chọn một giải pháp bảo mật Oracle, các khía cạnh cần được xem xét và cân nhắc: khả năng đáp ứng của giải pháp, tính hiệu quả và lợi ích mà giải pháp đem lại.

1. **Một số giải pháp bảo mật Oracle**

**1. Tính năng bảo mật mặc định của Oracle**

**Tài khoản người dùng**: Khi bạn tạo tài khoản người dùng, bạn có thể bảo mật tài khoản bằng nhiều cách khác nhau. Bạn cũng có thể tạo cấu hình mật khẩu để đảm bảo chính sách mật khẩu an toàn hơn cho trang web của mình.

**Phương thức xác thực** :Cơ sở dữ liệu Oracle cung cấp một số cách để định cấu hình xác thực cho người dùng và quản trị cơ sở dữ liệu. Ví dụ: bạn có thể xác thực người dùng ở cấp cơ sở dữ liệu, từ hệ điều hành và trên mạng.

**Đặc quyền và vai trò** :Bạn có thể sử dụng đặc quyền và vai trò để hạn chế quyền truy cập của người dùng vào dữ liệu.

**Bảo mật ứng dụng** :Bước đầu tiên để tạo một ứng dụng cơ sở dữ liệu là đảm bảo rằng nó được bảo mật đúng cách.

**Sử dụng ngữ cảnh ứng dụng trong phiên làm việc của người dùng**: Ngữ cảnh ứng dụng là cặp tên-giá trị chứa thông tin về phiên làm việc của người dùng. Bạn có thể truy xuất thông tin phiên về người dùng, chẳng hạn như tên người dùng hoặc thiết bị đầu cuối và hạn chế quyền truy cập cơ sở dữ liệu và ứng dụng cho người dùng đó dựa trên thông tin này.

**Sử dụng Cơ sở dữ liệu riêng ảo** **để truy xuất vào từng hàng và cột Database**: Một Cơ sở dữ liệu ảo bảo mật sẽ tự động nhúng một vị từ WHERE vào các câu lệnh SQL mà người dùng đưa ra.

**Mã hóa** : Bạn có thể ngụy trang dữ liệu trên mạng để ngăn chặn truy cập trái phép vào dữ liệu đó.

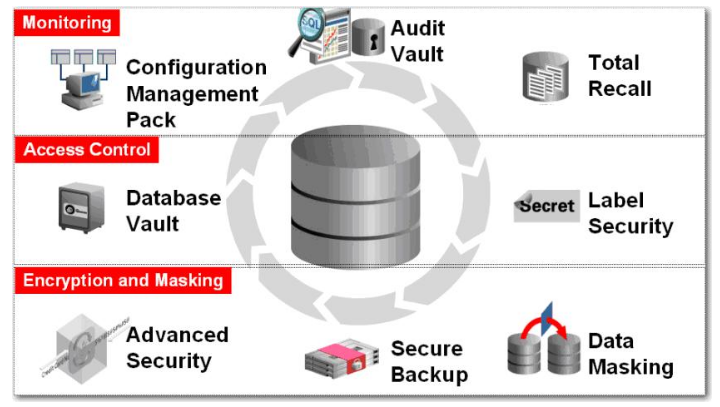
**Kiểm tra hoạt động cơ sở dữ liệu**: Bạn có thể kiểm tra các hoạt động cơ sở dữ liệu theo các thuật ngữ chung, chẳng hạn như kiểm tra tất cả các câu lệnh SQL, các đặc quyền SQL, các đối tượng lược đồ và hoạt động mạng. Hoặc, bạn có thể kiểm tra một cách chi tiết, chẳng hạn như khi các địa chỉ IP từ bên ngoài mạng công ty đang được sử dụng.

**2. Giới thiệu kiến trúc bảo mật Oracle Defense In Dept**

Kiến trúc “Defense-In-Dept” bảo vệ dữ liệu theo chiều sâu, sẽ theo dõi toàn bộ vòng đời của dữ liệu như:

* Ai có quyền truy cập vào dữ liệu và với điều kiện là gì?
* Đảm bảo hệ thống được cấu hình và duy trì theo các phương pháp trên
* Vị trí của dữ liệu
* Ứng dụng nào đăng nhập vào dữ liệu

Ba thành phần chính của kỹ thuật này là: Mã hóa và che dấu dữ liệu , theo dõi hoạt động người dùng và kiểm soát truy cập.



Kiến trúc bảo mật Defense in Dept

**Mã hóa và che giấu dữ liệu:**

 Các giải pháp mã hóa và che giấu dữ liệu đóng vai trò quan trọng trong bảo mật Oracle để bảo vệ dữ liệu bên trong doanh nghiệp. Dữ liệu trên các ổ đĩa bên dưới cơ sở dữ liệu và ứng dụng, dữ liệu trong môi trường thử nghiệm và phát triển, dữ liệu trên đường truyền và các bản sao lưu phục hồi sẽ được bảo vệ với các giải pháp mã hóa và che giấu dữ liệu. Việc di chuyển dữ liệu sản xuất sang nơi khác để phục vụ cho việc phát triển và thử nghiệm có thể dẫn đến tình trạng dữ liệu quan trọng lọt vào tay người dùng không nên biết. Bên cạnh đó, dữ liệu trên đường truyền cũng có thể bị đánh cấp bởi những người có ý đồ xấu. Với các giải pháp mã hóa và che giấu dữ liệu sẽ đảm bảo dữ liệu an toàn trên hệ thống, đường truyền và cả các bản sao lưu trong trường hợp bị mất hoặc rơi vào tay người dùng có ý đồ xấu

**Theo dõi hoạt động người dùng:**

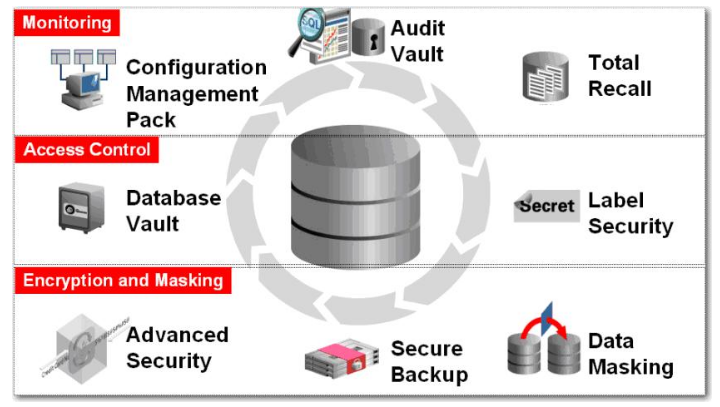
 Trong khi mã hóa và kiểm soát truy cập là những thành phần quan trọng để bảo vệ dữ liệu, nhưng những hoạt động đó là chưa đủ để đảm bảo an toàn bảo mật dữ liệu. Việc theo dõi các hoạt động của Database sẽ cho phép theo dõi các hoạt động của người dùng, các đối tượng của database được cấu hình mã hóa, che giấu và kiểm soát truy cập.Việc này cho phép phát hiện và xử lý kịp thời các hoạt động có ý đồ xấu.

**Kiểm soát truy cập:**

 Kiểm soát việc truy cập vượt quá mức cho phép của ứng dụng dụng hoặc người dùng vào Database là quan trọng, nhằm tạo điều kiện cho tổ chức đạt được những lợi ích của việc hợp nhất dữ liệu và điện toán đám mây. Bên cạnh đó, công việc đòi hỏi việc phân tách nhiệm vụ giữa những người dùng kể cả những người quản trị, kiểm soát việc đăng nhập sẽ giới hạn việc truy cập và các hoạt động của người dùng trên các dữ liệu có tính nhạy cảm và quan trọng.

**2.1. Giải pháp bảo mật Oracle Database Defense in Dept:**

Giải pháp bảo mật toàn diện Oracle Database đảm bảo an toàn bảo mật cho hệ thống Oracle Database một cách toàn vẹn và minh bạch, dựa trên kỹ thuật bảo vệ theo chiều sâu Defense-in-Dept với 3 phương pháp: mã hóa và che giấu dữ liệu, quản lý truy cập và theo dõi hoạt động người dùng. Do đó sẽ đảm bảo giải quyết được các vấn đề bảo mật trong môi trường doanh nghiệp hiện nay.



**Mã hóa và che giấu dữ liệu - Encryption and Masking**

* Giải pháp Secure Backup: mã hóa các dữ liệu sao lưu bao gồm database, các tập tin dữ liệu.
* Giải pháp Advanced Security: cung cấp khả năng mã hóa dữ liệu trên hệ thống và đường truyền.
* Giải pháp Data Masking: che giấu dữ liệu nhạy cảm trước khi chuyển cho nhân viên lập trình hoặc đối tác.

**Quản lý truy cập - Acess Control:**

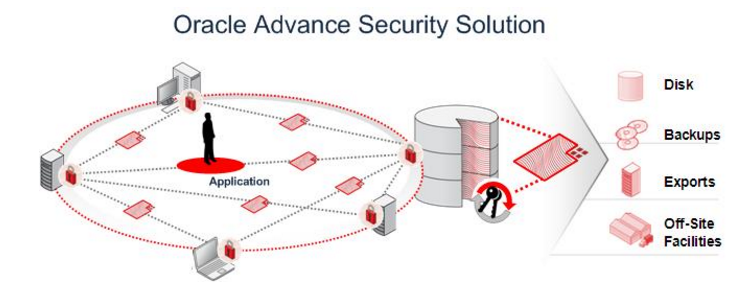
* Giải pháp Oracle Database Vault: kiểm soát,ngăn chặn các hoạt động của người dùng kể cả người quản trị trên hệ thống dữ liệu.
* Giải pháp Oracle Label Security: giải pháp phân cấp dữ liệu dựa theo nghiệp vụ của người dùng.

**Theo dõi hoạt động người dùng - Monitor:**

* Giải pháp Audit Vault: hợp nhất dữ liệu theo dõi từ nhiều Database khác nhau, đồng thời cho phép tạo các báo cáo và cảnh báo khi có các hoạt động đáng nghi trên Database.
* Giải pháp Total Recall: cho phép theo dõi những thay đổi của các dữ liệu quan trọng vào các thời điểm trong quá khứ.
* Giải pháp Configuration Management: tìm kiếm các lỗ hổng bảo mật trên hệ thống, cảnh báo và khuyến cáo cách khắc phục cho người quản trị.

**2.2. Giải pháp Advanced Security**

Giải pháp bảo mật Oracle Advanced Security cung cấp các tính năng mã hóa và chứng thực mạnh mẽ cho hệ thống Database Oracle, bảo vệ dữ liệu Oracle quan trọng ngay cả khi có sự xâm nhập trái phép trên đường truyền, hệ điều hành hoặc ngay cả khi thiết bị phần cứng, các bản sao lưu bị mất. Ngoài ra, giải pháp còn cung cấp các tính năng chứng thực mạnh mẽ như Kerberos, Radius, PKI.



**Lợi ích giải pháp**

Giải pháp bảo mật Oracle Advanced Security giúp người dùng đạt được những yêu cầu tuân thủ các quy định bảo mật bằng cách bảo mật dữ liệu quan trọng trên đường truyền, các ổ đĩa sao lưu và dữ liệu database không bị thất thoát ngay cả khi bị mất. Một số lợi ích của giải pháp:

* Mã hóa dữ liệu trên đường truyền
* Hiệu suất cao
* Cung cấp các chuẩn mã hóa cao cấp : AES, 3DES, X.509
* Mã hóa dữ liệu các cột trong bảng hoặc toàn bộ tablespace.
* Mã hóa dữ liệu mà không cần phải thay đổi ứng dụng

- Cho phép quản lý các key được tích hợp sẵn

- Được tích hợp với công cụ sao lưu RMAN, cho phép mã hóa dữ liệu sao lưu.

2.3. Giải pháp bảo mật Oracle Data Masking

Giải pháp bảo mật Oracle Data Masking cho phép doanh nghiệp chia sẻ dữ liệu sản xuất với các bộ phận nội bộ hoặc đối tác nhưng vẫn đảm bảo những dữ liệu nhạy cảm không bị tiết lộ. Data Masking sẽ thay thế các dữ liệu nhạy cảm trong database bằng dữ liệu tinh chế trong giống dữ liệu thật, dựa theo các quy tắc mặt nạ. Hội đồng kiểm soát chất lượng có thể dùng dữ liệu này để kiểm tra ứng dụng và thử nghiệm các mô hình hệ thống mà không vi phạm các chính sách hoặc luật pháp.



Lợi ích từ giải pháp bảo mật Oracle Data Masking:

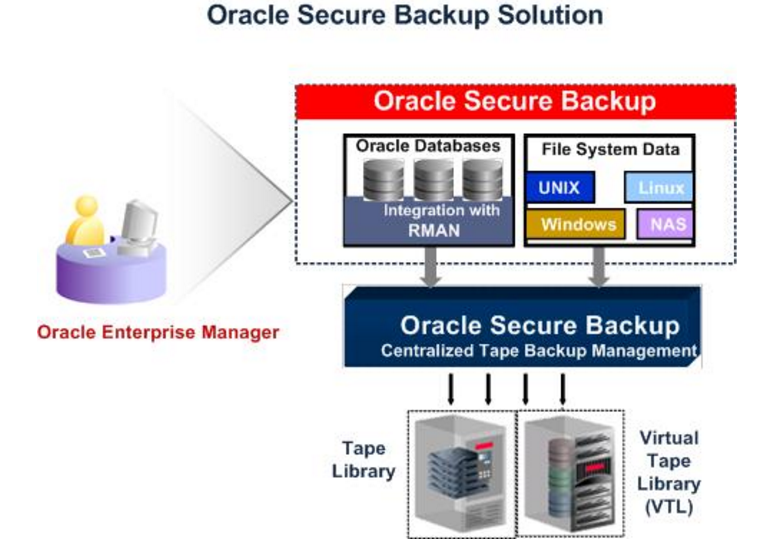
Chia sẻ dữ liệu sản xuất nhưng vẫn đảm bảo tuân thủ các quy định bảo mật dữ liệu của doanh nghiệp.

Cho phép thực thi các chính sách bảo mật dữ liệu đồng nhất và tự động xuyên suốt doanh nghiệp.

Hỗ trợ tìm kiếm các vùng dữ liệu nhạy cảm cần được bảo vệ, giúp tăng hiệu quả đối với người quản trị.

Giải pháp bảo mật Oracle Secure Backup

Việc quản lý dữ liệu sao lưu trên các máy chủ, các trung tâm dữ liệu và các văn phòng từ xa đòi hỏi một giải pháp sao lưu hợp nhất, cho phép giải quyết những khó khăn của môi trường dữ liệu phân tán. Giải pháp Oracle Secure Backup với kiến trúc client-server hỗ trợ khả năng mở rộng cao, cung cấp một giao diện quản lý các ổ đĩa tập trung cho toàn bộ hệ thống Công Nghệ Thông Tin của doanh nghiệp.



Lợi ích từ giải pháp bảo mật Oracle Secure Backup

Cho phép mã hóa không những dữ liệu mà còn cả những thiết bị phần cứng.

Cho phép sao lưu các tập tin hệ thống: Unix, Linux, Windows và các ổ đĩa NAS.

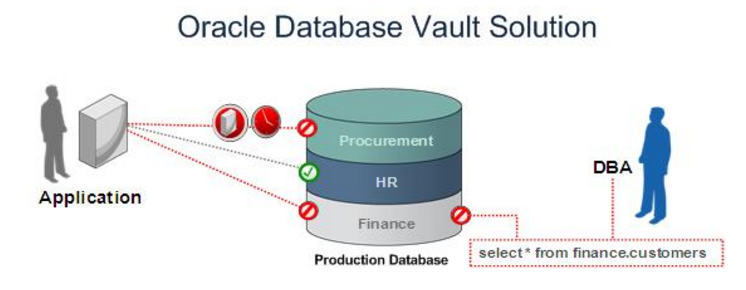
Quản lý dễ dàng và tập trung với công cụ sao lưu RMAN và quản lý Enterprise Manager.

Các tiến trình sao lưu dữ liệu đến các ổ đĩa tape nhanh và hiệu quả.

Quản lý việc sao lưu theo các chính sách, đảm bảo dễ dàng, tập trung và bảo mật.

2.4. Giải pháp bảo mật Oracle Database Vault

Kiểm tra việc truy cập vào database, ứng dụng và dữ liệu đòi hỏi việc kiểm soát truy cập tinh vi và chặt chẽ. Giải pháp Oracle Database Vault là giải pháp hàng đầu trong việc bảo vệ dữ liệu nhạy cảm của doanh nghiệp, cho phép kiểm soát việc truy cập vào dữ liệu của Database tuân thủ các chính sách mà không cần thay đổi trên ứng dụng. Oracle Database Vault sẽ ngăn cản những tài khoản có quyền truy xuất vào dữ liệu hoặc dùng các công cụ để thay đổi dữ liệu ứng dụng. Oracle Database Vault sẽ áp các chính sách bảo mật dữ liệu: người dùng được truy cập bằng phần mềm nào, khi nào và trên ứng dụng nào.



Lợi ích của giải pháp bảo mật Oracle Database Vault:

Phân tách vai trò giữa các người dùng trong Database, kể cả người quản trị.

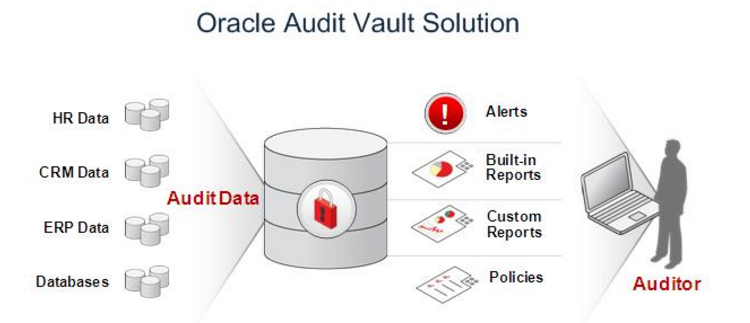
Hỗ trợ kiểm soát theo thời gian thực.

Kiểm soát ngăn chặn những người dùng có quyền truy cập vào dữ liệu nhạy cảm.

Hỗ trợ bảo mật ứng dụng với các chính sách được xây dựng từ Oracle.

2.5. Giải pháp bảo mật Oracle Audit Vault

Giải pháp bảo mật Oracle Audit Vault tự động hóa việc hợp nhất dữ liệu theo dõi thành một kho lưu trữ dữ liệu theo dõi, được bảo mật theo công nghệ của Oracle, cho phép theo dõi và báo cáo các hoạt động người dùng trên các Database một cách tập trung. Audit Vault cung cấp một kho thông tin theo dõi, các mẫu báo cáo được xây dựng sẵn, đồng thời tích hợp khả năng cảnh báo các sự kiện trong Database và phân tách theo vai trò của người dùng. Ngoài ra việc theo dõi trên Database Oracle, Audit Vault còn cho phép theo dõi Database của các hãng thứ ba như: IBM DB2, Microsoft SQL Server 2005, Sybase ASE.



Lợi ích từ giải pháp:

Tích hợp các bản báo cáo được xây dựng sẵn, tuân thủ các chính sách bảo mật và Atheo dõi.

Hợp nhất và bảo mật dữ liệu theo dõi các Database như Oracle, Mircosoft SQL Server, IBM BD2, Sysbase.

Tự động xóa dữ liệu theo dõi trên Database nguồn.

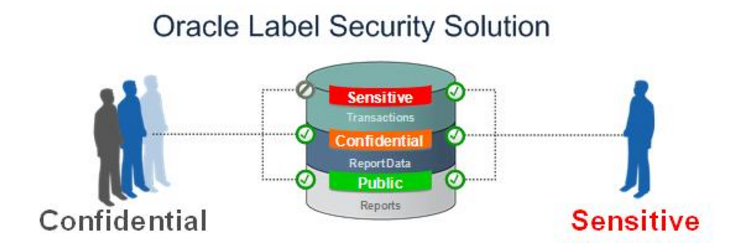
Hỗ trợ quản lý các chính sách bảo mật trên nhiều Database tập trung.

Gửi các cảnh báo cho người quản trị khi có các hoạt động đáng nghi trên Database.

Thu thập các giá trị từ các tập tin logs của các phiên giao dịch.

2.6. Giải pháp bảo mật Oracle Label Security

Ngày nay, việc kiểm soát chặt chẽ các hoạt động truy xuất dữ liệu ngày càng trở nên quan trọng , được đánh giá là tiêu chí hàng đầu của doanh nghiệp trong việc đảm bảo hợp nhất dữ liệu, tuân thủ các chính sách bảo mật. Việc duy trì những dữ liệu quan trọng theo từng Database riêng biệt đối với từng khách hàng sẽ tốn kém nhiều chi phí và làm tăng tải cho người quản trị. Tuy nhiên việc hợp nhất dữ liệu lại làm giảm đi tính bảo mật của hệ thống. Giải pháp bảo mật Oracle Label Security cung cấp khả năng phân tách dữ liệu theo vai trò của người dùng. Với khả năng này cho phép doanh nghiệp có thể lưu trữ những dữ liệu nhạy cảm với các dữ liệu khác trên một bảng dữ liệu nhưng vẫn đảm bảo tính bảo mật.



Lợi ích của giải pháp:

Phân cấp dữ liệu theo vai trò của người dùng với kỹ thuật dán nhãn dữ liệu.

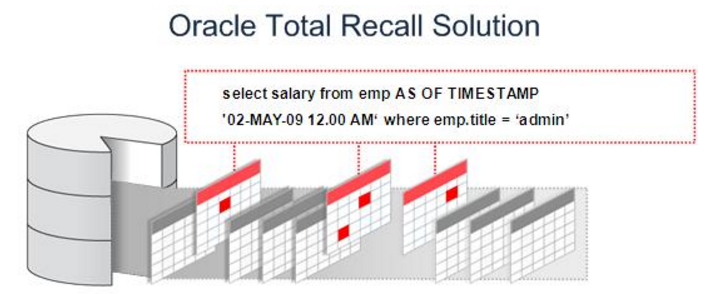
Áp dụng các chính sách, cho phép kiểm soát một cách dễ dàng và uyển chuyển.

Tích hợp với công cụ quản lý Enterprise Manager, cho phép quản lý tập trung.

Giao diện ứng dụng hoàn chỉnh với các chức năng bao gồm quản lý các chính sách, so sách và phân tích nhãn dữ liệu.

2.7. Giải pháp bảo mật Oracle Total Recall

Các tổ chức ngày nay cần một hệ thống hữu hiệu cho việc duy trì dữ liệu quá khứ trong một thời gian dài mà không cần phải viết lại ứng dụng hoặc các giải pháp phần mềm của hãng thứ 3, đồng thời không làm tăng tải việc quản trị. Giải pháp bảo mật Oracle Total Recall là lời giải cho các vấn đề này, bằng việc cung cấp hoàn chỉnh việc quản lý, bảo mật, duy trì tất cả dữ liệu trong quá khứ



Lợi ích giải pháp:

Truy xuất dữ liệu quá khứ nhưng không ảnh hưởng đến ứng dụng.

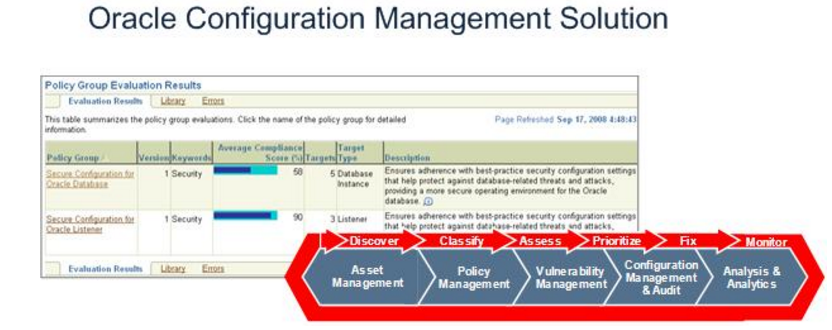
Doanh nghiệp không cần đến các giải pháp của hãng thứ 3.

Bảo mật dữ liệu quá khứ tuân theo các chính sách bảo mật.

Quản lý hiệu quả và tiết kiệm chi phí lưu trữ dữ liệu quá khứ.

2.8. Giải pháp bảo mật Oracle Configuration Management

Ngày nay,quản lý thông tin cấu hình của hệ thống là một trong những hoạt động quan trọng của bộ phận IT của doanh nghiệp. Với giải pháp Oracle Configuration Management cho phép quản lý thông tin cấu hình và tự động hóa các tác vụ IT. Giải pháp bảo mật Oracle Configuration được tích hợp với Oracle Enterprise Manager với khả năng tự động tìm kiếm, xác thực và báo cáo những thay đổi thông tin cấu hình trên hệ thống



Lợi ích từ giải pháp:

Tích hợp với công cụ quản lý Enterprise Manager, cho phép quản lý dễ dàng và tập trung.

Cung cấp các bản báo cáo tuân thủ các chính sách bảo mật.

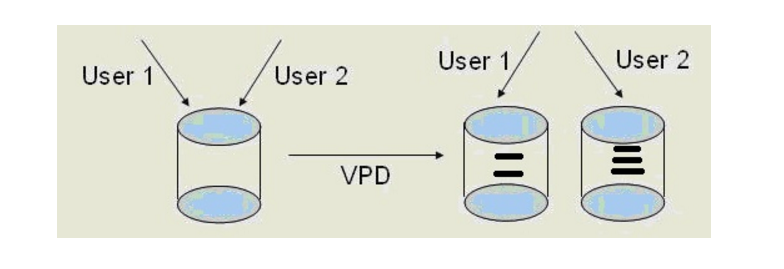
Ngăn chặn và phát hiện những thay đổi cấu hình không đúng.

2.9. Giải pháp Bảo mật CSDL riêng ảo trên Oracle

Bảo mật CSDL Oracle riêng ảo là một cơ chế bảo mật Oracle, cho phép ta tạo các chính sách bảo mật để điều khiển việc truy cập ở mức hàng, cột. Bản chất thì VPD thêm một mệnh đề WHERE vào câu lệnh SQL được đưa ra đối với bảng (table), khung nhìn (view) hoặc synonym (tên thay thế cho các đối tượng như bảng, khung nhìn, các thủ tục được lưu và các đối tượng CSDL khác).

VPD cung cấp giải pháp bảo mật tới mức mịn trực tiếp trên các table, view, synonym. Nó gán trực tiếp các chính sách bảo mật lên các đối tượng CSDL, và các chính sách sẽ tự động được thực hiện mỗi khi có một người dùng truy nhập dữ liệu đến các đối tượng đó.

Khi người dùng trực tiếp hoặc gián tiếp truy cập tới table, view hay synonym được bảo vệ bởi chính sách VPD, thì hệ thống CSDL Oracle sẽ tự động sửa lại câu truy vấn SQL của người dùng bằng cách thêm vào một mệnh đề WHERE. Biểu thức đằng sau mệnh đề WHERE thường được gọi là một tân từ (predicate) và thực hiện trong suốt đối với người dùng. Kết quả là mỗi người dùng có một khung nhìn khác nhau với CSDL ban đầu, tùy thuộc vào đặc quyền của họ.

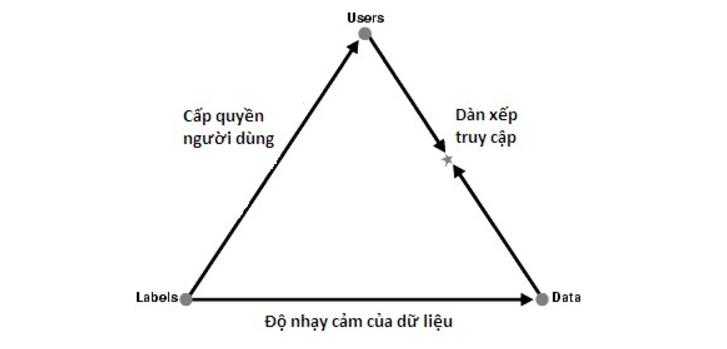


VPD kết hợp hai tính năng: chính sách kiểm soát truy cập mịn (Fine-grained) và ngữ cảnh ứng dụng (application context). Chính sách kiểm soát truy cập mịn cho phép xây dựng các ứng dụng hay chính sách bảo mật với mức chi tiết mịn. Các chính sách này cũng được gọi là chính sách VPD. Chẳng hạn, có thể dùng chính sách này để hạn chế khách hàng truy cập vào một máy chủ CSDL Oracle, họ chỉ được xem những tài khoản riêng của mình. Một bác sĩ chỉ có thể nhìn thấy các hồ sơ bệnh nhân của mình, hoặc một người quản lý chỉ có thể nhìn thấy các hồ sơ của nhân viên làm việc trong phòng của anh ta.

Có thể nói, VPD mang lại rất nhiều lợi ích trong việc bảo mật CSDL trong hệ quản trị Oracle. Bên cạnh đó cũng có thể được kết hợp với các cơ chế an toàn khác để đảm bảo an toàn mức cao cho CSDL.

3. Giải pháp bảo mật dựa vào nhãn trên Oracle

An toàn dựa vào nhãn là một cơ chế, cho phép kiểm soát truy cập theo mức hàng (row\_level), dựa trên cơ chế VPD của Oracle. Nó kiểm soát truy cập vào nội dung của một hàng bằng cách so sánh nhãn (label) của hàng với nhãn của người dùng và những đặc quyền của họ. Hình vẽ dưới đây thể hiện mối quan hệ giữa người dùng, dữ liệu và các nhãn.



Khi áp dụng chính sách OLS, một cột mới sẽ được thêm vào mỗi hàng dữ liệu. Cột này sẽ lưu trữ các nhãn phản ánh sự nhạy cảm của mỗi hàng dữ liệu trong CSDL. Khi đó có thể xác định được mức độ truy cập của người dùng vào CSDL bằng cách so sánh nhãn của người dùng với nhãn của hàng.

Lưu ‎ý rằng, nhãn cho phép chúng ta điều khiển truy cập mịn bằng cách dùng dữ liệu trong hàng. Mỗi nhãn dữ liệu sẽ chứa thông tin về mức độ nhạy cảm của dữ liệu. Nó là 1 thuộc tính đơn gồm 3 thành phần:

Level (thành phần bắt buộc) là thành phần phân cấp biểu thị độ nhạy cảm của dữ liệu, chẳng hạn: HIGHLY\_SENSITIVE, SENSITIVE, CONFIDENTIAL, PUBLIC. Đối với mỗi level, ta cần định nghĩa 1 dạng số (numeric form) và 2 dạng chuỗi (chuỗi dài- long form và chuối ngắn – short form).

Compartment (thành phần tùy chọn) là thành phần không phân cấp giúp phân lớp dữ liệu chính xác hơn, việc phân loại dữ liệu được phân chia theo lĩnh vực, chuyên ngành, dự án,.… Tức là nếu ta có 2 dữ liệu thuộc 2 compartment C1 và C2, thì có nghĩa là 2 dữ liệu đó thuộc 2 lĩnh vực khác nhau là C1 và C2 và không có nghĩa dữ liệu thuộc C1 nhạy cảm hơn dữ liệu thuộc C2 (hay ngược lại).

Group (thành phần tùy chọn) biểu diễn mối quan hệ sở hữu (thông thường nó thể hiện cơ cấu của công ty). Do vậy group có cấu trúc cây phân cấp “cha – con”. Một user có nhãn chứa một group cha thì có thể truy xuất dữ liệu thuộc group cha và tất cả các group con của group cha đó.

Trong Oracle, ta có thể thực thi OLS bằng công cụ Oracle Policy Manager. Tại đây, ta có thể tạo các chính sách OLS để áp dụng vào các bảng và các lược đồ.

Đối với một bảng được bảo vệ bởi một chính sách OLS, người dùng muốn truy cập vào một hàng, đòi hỏi nhãn của họ phải thỏa mãn một số tiêu chuẩn đã được định nghĩa trước trong chính sách đó. OSL cung cấp khả năng kiểm soát linh hoạt quyền truy cập vào dữ liệu nhạy cảm và kiểm soát truy cập dữ liệu dựa trên danh tính và nhãn của người dùng, sự nhạy cảm và nhãn của dữ liệu. Nó làm mịn thêm các điều khiển truy cập tùy ý, các điều khiển truy cập tùy ý này xác định hoạt động nào người dùng có thể thực hiện trên dữ liệu trong một đối tượng CSDL như: bảng hoặc khung nhìn.

Chính sách bảo mật Oraacle dựa vào nhãn là một cơ chế dựa trên kiểm soát bắt buộc (Mandatory Access Control - MAC, một loại chính sách kiểm soát truy cập trong CSDL). Do vậy, OLS có khả năng đảm bảo tính an toàn cao cho dữ liệu nhạy cảm, tuy nhiên việc thực thi và áp dụng OLS trên một hệ thống CSDL Oracle là khá phức tạp.

1. **Kết luận**

Việc bảo mật an toàn cho CSDL Oracle luôn là một việc vô cùng quan trọng. Tuy nhiên, bảo mật như thế nào lại là một vấn đề không hề đơn giản. Với những nội dung được trình bày trên, chúng ta có thể thấy rằng bên trong các hệ quản trị CSDL Oracle luôn có các cơ chế an toàn được hỗ trợ sẵn. Các cơ chế an toàn trong hệ quản trị Oracle có thể hỗ trợ trong việc bảo vệ CSDL Oracle. Các giải pháp trên có thể là một gợi ‎ý tốt cho các nhà quản trị an toàn khi cần thiết lập các biện pháp để bảo vệ CSDL

***Nguồn: http://www.wecommit.com.vn/giai-phap/bao-mat-oracle***