|  |
| --- |
| HỌC VIỆN KỸ THUẬT MẬT MÃ  **KHOA CÔNG NGHỆ THÔNG TIN**  Logo HvKTMM  **Bài tập lớn**  **Cơ sở an toàn thông tin**  **Đề tài :**  **Tìm hiểu về Real Application Security (RAS)**  **trong APEX**  Sinh viên thực hiện: VŨ THÀNH ĐẠT AT150314  MAI VĂN KHÁ AT150327  LÊ VĂN THẮNG AT150351  DƯƠNG QUANG HUY AT150323  Nhóm 8  Giảng viên hướng dẫn: Trần Nghi Phú    Hà Nội, 09-2021 |

**BAN CƠ YẾU CHÍNH PHỦ**

**HỌC VIỆN KỸ THUẬT MẬT MÃ**

**KHOA: AN TOÀN THÔNG TIN**

**🙟🕮🙝**

**AN TOÀN CƠ SỞ DỮ LIỆU**

**Tìm hiểu về Real Application Security (RAS)**

**trong APEX**

Nhận xét của giáo viên hướng dẫn:

Điểm báo cáo:

**Xác nhận của giáo viên hướng dẫn:**

**MỤC LỤC**

[Chương 1 : Mở đầu 4](#_Toc83224671)

[**1.1 Lí do chọn đề tài 4**](#_Toc83224672)

[**1.2 Mục đích 4**](#_Toc83224673)

[Chương 2 : Tổng quan về Real Application Security 5](#_Toc83224674)

[**2.1 Real Application Security (RAS) 5**](#_Toc83224675)

[**2.1.1 Giới thiệu về Real Application Security (RAS) 5**](#_Toc83224676)

[**2.2 Các tính năng của RAS 5**](#_Toc83224677)

[**2.3 Ví dụ về Real Application Security 5**](#_Toc83224678)

[**2.4 Một số khái niệm về RAS 5**](#_Toc83224679)

[**2.4.1 Data Realms 5**](#_Toc83224680)

[**2.4.2 Policy Components 5**](#_Toc83224681)

[**2.5 Thiết lập với API PL / SQL 6**](#_Toc83224682)

[**2.6 Công cụ quản trị RAS 6**](#_Toc83224683)

[**2.7 Các tính năng Real Application Security 8**](#_Toc83224684)

[Chương 3 : Bảo mật APEX của Oracle 9](#_Toc83224685)

[**3.1 Khái niệm 9**](#_Toc83224686)

[**3.2 Kiểm soát truy cập 9**](#_Toc83224687)

[**3.4 Màn hình quản trị access control 10**](#_Toc83224688)

[**3.5 Những thách thức về kiểm soát truy cập 11**](#_Toc83224689)

[Chương 4 : RAS trong APEX 11](#_Toc83224690)

[**4.1 Tích hợp RAS với APEX 11**](#_Toc83224691)

[**4.2 Tích hợp RAS với APEX 12**](#_Toc83224692)

[**4.3 DEMO RAS trong APEX 13**](#_Toc83224693)

[**4.4 Lợi ích của RAS 13**](#_Toc83224694)

[Chương 5 : Kết luận 14](#_Toc83224696)

[Chương 6 : Tài liệu thâm khảo 14](#_Toc83224697)

**LỜI MỞ ĐẦU**

Trong những thập kỷ gần đây, thế giới và Việt Nam đã và đang chứng kiến sự phát triển và bùng nổ của Công nghệ thông tin và Truyền thông. Cùng với sự phát triển ấy là vai trò ngày càng quan trọng của cơ sở dữ liệu khi xã hội chuyển sang giai đoạn xã hội hóa thông tin và kinh tế hóa thông tin với quy mô toàn cầu. Chính vì vậy, vấn đề uỷ quyền, vấn đề truy cập, bảo mật thông tin trong cơ sở dữ liệu đang là một thách thức đối với các doanh nghiệp, tổ chức.

Cũng chính vì vậy, Oracle Database Real Application Security (RAS) là một giải pháp cấp quyền cho doanh nghiệp. Nó được thiết kế để cung cấp ủy quyền ứng dụng và bảo mật dữ liệu (VPD) bất kể phương thức truy cập. tức là APEX, Java, PHP, Perl, .NET, DB trực tiếp, v.v.

Mục đích chọn đề tài “Tìm hiểu về Real Application Security (RAS) trong APEX” của chúng em là nghiên cứu về RAS trong APEX, tìm hiểu các thành phần của nhãn và các chính sách áp dụng trong RAS. Dựa những kiến thức đã tìm hiểu được thực hiện áp dụng RAS vào cơ sở dữ liệu.

Hơn nữa, việc thực hiện đề tài này sẽ một phần nào đó hỗ trợ chúng em trong việc định hướng việc làm và giúp chúng em có được thêm những kiến thức nền tảng và bổ ích để phục vụ cho công việc sau này.

# Chương 1 : Tổng quan về Real Application Security

## **1.1 Real Application Security (RAS)**

### **1.1.1 Khái niệm về Real Application Security (RAS)**

Real Application Security (RAS) là một giải pháp cấp quyền

- Hỗ trợ Declarative Security Policies

- Cung cấp khả năng đảm bảo an toàn đầu-cuối (end-to end) cho các ứng dụng nhiều lớp

- Cung cấp giải pháp tích hợp để bảo vệ cơ sở dữ liệu và tài nguyên ứng dụng

- Nâng cấp cấu trúc an toàn của Oracle Database để đáp ứng nhu cầu cho việc phát triển các ứng dụng internet

## **1.2 Các tính năng của RAS**

- Hỗ trợ các Application User (Người dùng ứng dụng) và Application Sessions (Phiên làm việc ứng dựng)

- Hỗ trợ Application Privileges (Đặc quyền ứng dụng) và Application Roles

(Role của ứng dụng)

- Hỗ trợ sàng lọc dữ liệu chi tiết đến từng hàng, từng cột

## **1.3 Ví dụ về RAS (Real Application Security)**

- User DAUSTIN có thể xem được các bản ghi của các nhân viên thuộc IT department trong bảng EMPLOYEES nhưng không thể xem được thông tin về lương trong bản ghi đó

- Tất cả user có thể xem được toàn bộ thông tin của chính mình trong bảng EMPLOYEES

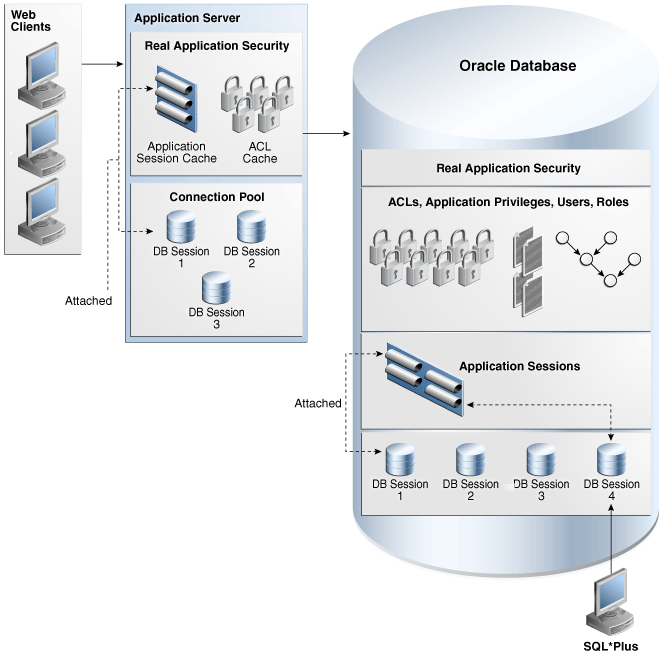
Hình 2.3: View của DAUSTIN trong bảng EMPLOYEES

Graphical user interface

Description automatically generated

## **1.4 Kiến trúc RAS**

RAS được quản lý thông qua một bộ các PL/SQL và các Java APIs. Cấu trúc này cho phép chúng ta cấu hình chi tiết các bộ phận của RAS bao gồm Application User (Người dùng ứng dụng), Application Role (Role của ứng dụng), Sessions (các phiên làm việc) và các bộ phần khác có liên quan.



## **1.5 Một số khái niệm về RAS**

### **1.5.1 RAS Data Realms**

Data Realm là một nhóm các hàng (record) biểu diễn cho một đối tượng nào đó trong cơ sở dữ liệu.

Ví dụ: Toàn bộ nhân viên trong bảng EMPLOYEES

Các nhân viên thuộc bộ phận IT department

Các nhân viên dưới quyền quản lý của 1 quản lý nào đó

Có thể cấp Privilege (Đặc quyền) cho các cột trong một Data Realm

Ví dụ: Xem cột Lương

Xem cột Số điện thoại

### **1.5.2 RAS Data Security Policy**

Để bảo vệ các dữ liệu trong một bảng, chúng ra cần định nghĩa một Data Security Policy. Từ đó chúng ta có thể bảo vệ các Record cả ở mức hàng và mức cột.

Data Security Policy thực hiên các chức năng sau đây:

- Xác định cụ thể dữ liệu cần bảo vệ (xác định Realm)

- Kết nối các Realm đã được xác định với một ACL(Access Control List) để xác định rõ các Privilege (Đặc quyền) đối với dữ liệu, các User/Role được cấp những đặc quyền đó

Hình 1.5.2: Ví dụ về một Access Control List

Diagram

Description automatically generated

# Chương 2 : Cài đặt RAS

*Lưu ý: toàn bộ các bước cài đặt này được thực hiên trên Schema HR được cài đặt làm demo trên Oracle 19c, và được thực thi bằng 1 User có quyền quản lý RAS và các quyền cần thiết*

## **2.1 Tạo các role và user:**

### **2.1.1 Tạo các Role cần thiết:**

Text

Description automatically generated

## Text Description automatically generated

### **2.1.2 Tạo User và gán cho các Role cần thiết:**

## Text, letter Description automatically generated

## **2.2 Tạo Security Class và ACL:**

### **2.1.1 Tạo Security Class:**

Text

Description automatically generated

### **2.2.2 Tạo ACL:**

Text

Description automatically generated

## **2.3 Cài đặt Data security policy:**

### **2.3.1 Cài đặt Data security policy**

Text

Description automatically generated

**2.3.2 Áp dụng Data security policy vào bảng:**

Text

Description automatically generated

# Chương 3 : RAS( Real Application Security) trong APEX

## **3.1 Tổng quan về APEX**

## **3.1.1 Định nghĩa**

APEX (Oracle Application Express)  là một công cụ phát triển ứng dụng web nhanh chóng cho các cơ sở dữ liệu Oracle. Oracle Application Express kết hợp những phẩm chất của một cơ sở dữ liệu cá nhân, năng suất, dễ sử dụng, và tính linh hoạt với những phẩm chất của một cơ sở dữ liệu doanh nghiệp, bảo mật, toàn vẹn, khả năng mở rộng, tính sẵn có và xây dựng cho web. Application Express là một công cụ để xây dựng các ứng dụng dựa trên web và các môi trường phát triển ứng dụng cũng thuận tiện dựa trên web.

## **3.1.2 Hệ thống bảo mật của APEX**

Authentication Schemes

- Xác đinh phương thức đăng nhập – dựa trên User

Authorization Schemes

- Xác định các hành động được phép thực hiện trong ứng dụng – dựa trên Role

Hình 3.1.2: các thành phần của APEX security

Text

Description automatically generated with medium confidence

## **3.2 Tích hợp RAS với APEX**

- Application user được giám sát trong cơ sở dữ liệu

+ Việc định danh Application user được thực hiên tại APEX

- RAS session ( phiên Real Application Secuity) chứa thông tin về Application user, role của user đó và ngữ cảnh của phiên làm việc

+ Quá trình này được dựa trên ngữ cảnh của ứng dụng APEX

- Mã nguồn của ứng dụng APEX được thực hiện tại RAS session

+ RAS session được gắn với 1 DB session

Hình 3.2 Sơ đồ tích hợp RAS với APEX

Diagram

Description automatically generated

- APEX có thể sử dụng RAS user, role và Data security policy

 - RAS session được ra dựa trên một APEX session

## **3.3 Cài đặt RAS trong APEX**

### **3.3.1: Kích hoạt tính năng RAS tại APEX**

- Đăng nhập vào APEX bằng tài khoản ADMIN có quyền cao nhất

- Kích hoạt tính năng Real Application Security tại Manage Instance \ Security

Hình 3.3.1:

A screenshot of a computer

Description automatically generated with medium confidence

### **3.3.2. Cài đặt tính năng RAS tại ứng dụng cụ thể:**

- Đăng nhập vào Workplace nơi cài đặt ứng dụng cần kích hoạt RAS

- Bật RAS tại mục <Tên ứng dụng>\Shared Components\Authentication Schemes\Create / Edit

Hình 3.3.2:

A screenshot of a computer

Description automatically generated

# Chương 4 : Kết luận

## **4.1 Kết luận tổng quan về RAS**

RAS (Real Application Security) là một giải pháp cấp quyền hiệu quả, bảo mật cao, thích hợp cho các môi trường doanh nghiệp quy mô lớn, yêu cầu sự tập trung hoá về việc bảo mật, quản lý dữ liệu

## **4.2 Các lợi ích của việc sử dụng RAS**

- Tính bảo mật cao

+ Các chính sách bảo mật được áp dụng bất kể người dùng dùng ứng dụng nào: trực tiếp, APEX hoặc các ứng dụng middleware

+ Có các cơ chế kiểm toán end-user (người dùng cuối)

- Đơn giản hoá việc phát triển ứng dụng

- Quản lý truy cập hiệu suất cao

- Đơn giản hoá việc quản lý, thay vì phải quản lý chi tiết nhiều ứng dụng, quản trị viên chỉ cần quản lý RAS tại database

# Tài liệu tham khảo

1. Oracle [Database Real Application Security Administrator's and Developer's Guide](Database%20Real%20Application%20Security%20Administrator's%20and%20Developer's%20Guide)
2. Dimitri Gielis - Founder & CEO of APEX R&D [Real ApplicationSecurity (RAS) in APEX](https://www.doag.org/formes/pubfiles/8006204/2016-NN-Dimitri_Gielis-A_primer_on_RAS_in_APEX-Praesentation.pdf)