Oracle Database Security Overview for Sale

## Oracle Security Introduction

Giới thiêu:

* Có rất nhiều cuộc tấn công vào database từ cả trong lẫn ngoài. Ví dụ : ...
* Bảo mật là 1 vấn đề cần thiết
* Oracle database đã được tích hợp sẵn các tính năng bảo mật, nhưng vẫn còn tồn tại các lỗ hổng
* Bài giới thiệu gồm 2 phần:
  + **Database Feature:** Các tính năng tích hợp sẵn trong database
    - Users
    - Controlling access to data
    - Securing Data on Network
    - Audit
  + **Security Solution:** Các giải pháp tăng thêm tính bảo mật cho database
    - *Oracle Audit Vault and DB Firewall*
    - *Oracle DB Vault*
    - *Oracle Label Security*
    - *Oracle Secure Backup*
    - *Oracle Data Masking*
    - *Oracle Advanced Security*

## Database Feature

### Users

* Tính năng bảo mật cơ bản của database
  + Database bao gồm nhiều user, mỗi user sở hữu 1 schema riêng
  + Không thể truy cập vào schema của user khác nếu ko được cho phép
* Chỉ những User hợp lệ mới có thể truy cập database:
  + Unique username: tên của user
  + Password : mật khẩu
  + User profile : các chính sách được áp dụng cho user ( ngày hết hạn ...)
* User đặc biệt :
  + SYS, SYSTEM: có toàn quyền đối với hệ thống

### Controlling Access to Data

* **Kiểm soát luồng dữ liệu** trong database
* Bao gồm 3 công nghệ chính:
  + Virtual Private Database ( VPD): ảo hóa database
  + Application contexts: kiểm soát truy cập dữ trên điều kiện
  + Transparent Sensitive Data Protection: mã hóa 1 số thành phần của DB

### Securing The Network

* Bảo vệ các kêt nối tới database
* Mỗi database bao gồm ít nhất 1 **listener** là nơi tiếp nhận các thông tin tới database.
* Các cách thức bảo vệ listener:
  + Không cho phép truy cập từ xa vào listener
  + Sử dụng password khi truy cập listener
  + Tùy chỉnh port mặc định (1521)
  + Cấu hình thời gian timeout...

### Audit

* Theo dõi tất cả các thao tác được thực hiện trên database
* Các kiểu Audit:
  + Audit hệ thống
  + Audit các object
  + Audit Sysdba

### License

* Đề nghị sử dụng phiên bản **Enterprise Edition:**
  + Mua License theo **Named User Plus**
    - 950 $/ user
    - 209$ / user/year
  + Mua License theo **Processor**
    - 47500$/processor ( nhân hệ số phần cứng)
    - 10450$/processor/year ( nhân hệ số phần cứng)
    - **Đề nghị sử dụng**

## Security Solution

### Introduction

* Các tính năng tích hợp sẵn trong database có thể đảm bảo an toàn cho DB
* Tuy nhiên trong quá trình vận hành, tương tác với các thành phần khác trong hệ thống ( ứng dụng,mạng, storage...) thì lại xuất hiện các lỗ hổng
  + Tester
  + Lưu trữ các file dữ liệu, các file backup
* Oracle cung cấp các giải pháp để khắc phục những lỗ hổng này

### Oracle Audit Vault & Database Firewall

Audit Vault:

* Khái niệm: Công nghệ của Oracle cho phép thu thập và quản lý tất cả các thông tin của các hệ thống ( Oracle database, non- Oracle Database, Os)
* Mục đích:
  + Theo dõi và quản lý tập trung một cách thuận tiện
  + Tạo những cảnh báo cần thiết cho người quản trị
* Cơ chế hoạt động
  + Thu thập các file audit từ các databaes Oracle
  + Thu thập log từ các database/ hệ thống khác

FireWall:

* Khái niệm: Công nghệ của Oracle cho phép tạo 1 trạm kiểm soát nằm giữa ứng dụng và Database nhằm năm bắt, tạo cảnh báo hoặc ngăn chặn các cuộc tấn công tới database
* Mục đích:
  + Ngăn chặn các cuộc tấn công
  + Ghi lại log của các hoạt động truy cập tới DB
  + Cung cấp các tool tăng cường các tính năng bảo mật của DB hiện có như mã hóa dữ liệu và xác thực người dùng
* Cơ chế hoạt động
  + Hoạt động dựa trên các chính sách được cấu hình
  + Có khả năng tự học dựa trên các hành động đã xảy ra
* Price:
  + Processor License: 6000$ / processor
  + Software Update License & Support: 1320$ / year

### Oracle Database Vault

* Khái niệm: Công nghệ của Oracle cho phép tăng cường khả năng bảo mật cho database bằng cách kiểm soát truy cập của user tới các object trong database
* Mục đích:
  + Bảo đảm an toàn cho DB từ các cuộc tấn công từ bên trong.
* Cơ chế hoạt động
  + User nào chỉ được phép truy cập vào schema của user đó
  + SYS không được phép truy cập vào dữ liệu của user khác
  + Mọi gán quyền truy cập thông thường đều không có hiệu lực
  + Hệ thống phân chia quyền một cách rõ rang, bao gồm 3 user quản trị viên ngang hàng nhau:
    - Sys: quản lý hệ thống
    - Dbv: phân chia, kiểm soát truy cập của các user khác
    - Dbu : Tạo và xóa user
* Price:
  + Named User Plus: 230$ / user
  + Software Update License & Support ( Database): 50,6$

Hoặc

* + Processor License:11500$ /processor
  + Software Update License & Support: 2530$ / year

### Oracle Label Security

* Khái niệm: Công nghệ của Oracle cho phép tăng cường khả năng bảo mật cho database bằng cách kiểm soát truy cập của user tới các row trong các table trong database
* Mục đích:
  + Bảo đảm an toàn cho DB từ các cuộc tấn công từ bên trong.
* Cơ chế hoạt động:
  + Add vào mỗi row 1 trường mới ( label)
  + Kết hợp label của row và user
  + Đưa ra quyết định truy vấn
* Price:
  + Named User Plus: 230$ / user
  + Software Update License & Support ( Database): 50,6$

Hoặc

* + Processor License:11500$ /processor
  + Software Update License & Support: 2530$ / year

### Oracle Secure Backup

* Khái niệm: Công nghệ của Oracle nhằm tối ưu hóa công việc backup dữ liệu
* Mục đích:
  + Đảm bảo an toàn cho các dữ liệu backup.
* Cơ chế hoạt động
  + Vẫn sử dụng công nghệ RMAN
  + Sử dụng công nghệ Backup System file và Database file ra tape.
  + Mã hóa các file backup
  + Quản lý tập trung
* Price
  + License Price : 3500$
  + Software Update License & Support: 770$ / year
  + Licensing Metric: Per Tape Drive

### Oracle Data Masking

* Khái niệm: Công nghệ của Oracle cho phép hư cấu dữ liệu nhưng vẫn giữ nguyên cấu trúc, tính chất của dữ liệu.
* Mục đích:
  + Bảo vệ dữ liệu bị rò rỉ trong quá trình test của ứng dụng
* Cơ chế hoạt động:
  + Tạo ra database clone để tester làm việc
  + Cách ly tester với dữ liệu thật
  + Thay thế các dữ liệu thật bởi các dữ liệu hư cấu nhưng vẫn giữ nguyên cấu trúc dữ liệu
  + Cách thức thay thế: Oracle cung cấp sẵn
* Price:
  + Named User Plus: 230$ / user
  + Software Update License & Support ( Database): 50,6$

OR

* + Processor License:11500$ /processor
  + Software Update License & Support: 2530$ / year

### Oracle Advanced Security

* Khái niệm: Công nghệ của Oracle nhằm tăng cường khả năng bảo vệ cho database
* Mục đích:
  + Bảo vệ dữ liệu bằng cách ngăn chặn các hành vi truy cập không hợp lệ
* Cơ chế hoạt động:
  + Data Redaction:
    - Tương tự như Data Masking
    - Thực hiện ngay trên database
  + Transparent Data Encryption
    - Mã hóa toàn bộ database
* Price:
  + Named User Plus: 230$ / user
  + Software Update License & Support ( Database): 50,6$

OR

* + Processor License:11500$ /processor
  + Software Update License & Support: 2530$ / year