

SECURITATEA BAZELOR DE DATE ORACLE

Autor: Ecaterina NEMERENCO, studentă SI-141

Universitatea Tehnică a Moldovei, catedra Automatică și Tehnologii Informaționale

Abstract: *From the outset, Oracle has delivered the industry's most advanced technology to safeguard data at the source—the database. Oracle provides a comprehensive portfolio of security solutions to ensure data privacy, protect against insider threats, and enable regulatory compliance for both Oracle and non-Oracle databases. Oracle's powerful preventive and detective security controls include database activity monitoring and blocking, privileged user and multifactor access control, data classification and discovery, transparent data encryption, consolidated auditing and reporting, secure configuration management, and data masking.*

Cuvinte cheie: *Oracle Database, politici de securitate, user, roluri, privileger, backup, framework de securitate, manager recovery, audit, securitate.*

Introducere

Baza de date Oracle are o structură fizică și o structură logică. Deoarece structura logică și structura fizică sunt separate, structura fizică poate fi gestionată fără să afecteze accesul la structura logică.

Sistemele de baze de date multiutilizator, cum este Oracle, includ caracteristici de securitate care controlează cum accesează utilizatorii baza de date. De exemplu, mecanismele de securitate previn accesul neautorizat la baza de date, împiedică accesul neautorizat la obiectele schemei, controlează accesul la discurile de stocare, controlează folosirea resurselor sistemului (cum ar fi CPU) și auditează acțiunile utilizatorilor.

1. Framework de securitate

Un framework de securitate bine definit trebuie să se dezvolte prin implicarea părților interesate și trebuie să fie autoevaluat de-a lungul timpului de utilizare. Majoritatea organizațiilor înțeleg nevoia de a avea un framework bine organizat, creează unul, însă uită de necesitatea de-al dezvolta încontinuu.

Utilizatorii bazei de date și schemele

Fiecare baza de date Oracle are o listă cu numele utilizatorilor. Pentru a o accesa, un utilizator trebuie să folosească o aplicație și să încerce să se conecteze cu un nume valid de utilizator al bazei de date. Fiecare nume utilizator are asociată o parolă pentru a împiedica accesul neautorizat.

Securitatea domeniului

Fiecare utilizator are o securitate de domeniu, un set de proprietăți care determină: acțiunile (privilegiile și rolurile) disponibile utilizatorului, cota de spațiu (spațiul disponibil) pentru utilizator, limitele resurselor sistemului pentru fiecare utilizator (de exemplu: timpul de procesare VC).

Privilegiile

Privilegiile bazei de date Oracle pot fi divizate în două categorii distincte: privilegii sistem și privilegii ale obiectelor schemei.

Privilegiile sistem permit utilizatorilor să execute o acțiune particulară a sistemului sau o acțiune particulară într-un tip particular al schemei. De exemplu, privilegiul de a crea un spațiu în tabelă sau de a șterge rânduri din orice tabelă a bazei de date, este privilegiu sistem. Mai multe privilegii sistem sunt disponibile numai administratorului și dezvoltatorilor de aplicații deoarece aceste privilegii sunt foarte puternice.

Rolurile

Oracle furnizează o gestiune și control a privilegiilor prin intermediul rolurilor. Rolurile sunt grupuri de privilegii înrudite care sunt acordate utilizatorilor, grupurilor de utilizatori sau altor roluri.

Auditarea

Oracle permite auditul selectiv (monitorizarea înregistrată) a acțiunilor utilizatorului în ajutorarea investigării utilizării suspicioase a bazei de date. Auditul poate fi făcut la trei nivele diferite:

- auditul comenzii - este auditul specific comenzii SQL fără să privească un obiect specific numit de schema. Auditul comenzii poate fi extins să auditeze toți utilizatorii sistemului sau poate fi folosit pentru auditarea numai a utilizatorilor selectați ai sistemului.

- auditul privilegiului - este auditul celor mai puternice privilegii sistem fără să privească un nume de obiect specific din schemă. Poate fi extins să auditeze toți utilizatorii sau focalizat numai la utilizatori selectați.

- auditul obiectului schemei - este auditul accesului la un obiect specific al schemei fără să privească utilizatorii. Auditul obiectului monitorizează comenzile permise prin privilegiile obiectului cum ar fi comenzile SELECT sau DELETE pentru o tabela dată.

Managerul Recovery

Managerul Recovery este un utilitar Oracle care gestionează operațiile de salvare și restaurare, menține un catalog de refacere (recovery catalog) obligatoriu, care conține informații despre fișierele de back-up și fișierele arhivelog. Recovery Manager folosește recovery catalog pentru a automatiza operațiile de restaurare și refacere a suportului de înregistrare.

Recovery catalog conține: informații despre backup-urile fișierelor de date și fișierelor arhivelog, informații despre copiile fișierelor de date, informații despre fișierele redo, log arhivate și copiile acestora, informații despre schema fizică a bazei de date destinație, secvențe de comenzi numite stored scripts.

Concluzie

Amenințări de securitate și reglementarea sporită a informației cu caracter personal, date despre carduri de plată, înregistrările fișelor medicale și alte date sensibile au extins posibilitățile de criptare a datelor în centrul de date. Oracle Database vine și cu produse adiționale de securitate care pot fi procurate și care oferă caracteristici avansate de securitate a bazelor de date, printre ele se numără: Oracle Label Security, Oracle Database Vault, Oracle Audit Vault, Oracle Enterprise User Security etc..

Oracle Key Vault permite clienților să implementeze criptarea și alte soluții de securitate gestionate de cheile de criptare, cum ar fi: portofele electronice Oracle, Java Keystore și fișiere de acreditare. Oracle Key Vault este o platformă centralizată de management al cheilor, care accelerează criptarea datelor în întreprindere și pe cloud.

Bibliografie

1. Oracle Database Security. [Resursă electronică]. -Regim de acces: <https://www.oracle.com/database/security/index.html>
2. Soluții de securitate Oracle [Resursă electronică]. -Regim de acces: <http://www.oracle.com/us/technologies/security/overview/index.html>