

ORACLE DATABASE VAULT

A LEGFONTOSABB ELŐNYÖK

- Az alkalmazások adatainak védelme a DBA illetéktelen hozzáféréstől
- Az adatbázis védelme az alkalmazások rendszergazdáinak és erős jogosultságú felhasználóinak illetéktelen hozzáféréstől
- Az alkalmazás-hozzáférés rugalmas biztonsági beállításokkal való szabályozása
- Az adatbázisok védelme a nemkívánatos módosításoktól
- A felelősségi körök szétválasztásának érvényesítése
- Biztonsági kiegészítés az adatbázis-kezelőhöz: Oracle Database 10g Release 2 Enterprise Edition Security Option

Manapság a következő biztonsági problémák számítanak a legsúlyosabbnak: a vállalaton belüli veszélyforrásokkal szembeni védelem, a jogszabályi követelmények teljesítése és a felelősségi körök szétválasztásának érvényesítése. Az Oracle Database Vault ezekre kínál megoldást. Először is megakadályozza, hogy az adatbázis-adminisztrátor (DBA) lássa az alkalmazások adatait. Ez elsődleges szempont azoknál a szervezeteknél, ahol korlátozni kell a partnerek, alkalmazottak és vevők bizalmas, üzleti jellegű vagy személyes adataihoz való hozzáférést. Emellett megakadályozza, hogy a kiemelt jogosultságú alkalmazás-rendszergazdák és adatbázis-adminisztrátorok hozzáférjenek más alkalmazásokhoz, és a jogosultsági körükön kívül eső tevékenységet végezzenek. Az Oracle Database Vault gyorsan és könnyedén, funkcióik korlátozása nélkül védi meg a meglévő alkalmazásokat.

Miből áll az Oracle Database Vault?

Az Oracle Database Vault megoldást kínál jó néhány igen gyakori biztonsági problémára és belső veszélyforrásra:

- Korlátozza a DBA és más erős jogosultsággal rendelkező felhasználók hozzáférést az alkalmazások adataihoz
- Megakadályozza, hogy az alkalmazás rendszergazdája jogosulatlanul módosítsa az adatbázist, és hozzáférjen más alkalmazások adataihoz
- Pontosan szabályozhatóvá teszi, hogy ki, mikor és honnan érheti el az alkalmazásokat

A Sarbanes–Oxley-féle törvény, az egészségbiztosítás hordozhatóságáról és ellenőrizhetőségéről szóló amerikai törvény, a személyes adatok védelméről szóló japán törvény, az Európai Unió adatvédelmi és elektronikus kommunikációs irányelve, valamint a kaliforniai szenátus 1386. sz. törvénye más előírásokkal együtt megkövetelik a belső szabályozás szigorítását az érzékeny információk jogosulatlan felfedésének vagy módosításának megelőzésére, mert ezek a személyi azonosítók eltulajdonításához és pénzügyi szabálytalanságokhoz vezethetnek.

Korábban a DBA vagy az alkalmazás rendszergazdája korlátlanul hozzáférhetett az adatbázishoz, így az alkalmazás adataihoz és az adatszótárhoz is, mert ez leegyszerűsítette az alkalmazás megtervezését, kifejlesztését és terítését. Valóban nehéz, sőt, talán lehetetlen is a felhasználói környezet alapján kiegészítő hozzáférési szabályokat megadni anélkül, hogy alapos ismereteink lennének a kérdéses alkalmazás felépítéséről.

Az Oracle Database Vault egy sor új és professzionális biztonsági szolgáltatással rendelkezik, amelyek a Realms (tartományok), Factors (tényezők) és Rules (szabályok) fogalmain alapulnak. Segítségükkel még a legerősebb, pl. „SELECT ANY” jogosultsággal rendelkezők vagy a DBA-k hozzáférése is korlátozható. Mindezen funkciókat rugalmasan, az adott vállalati igényekhez alkalmazkodva lehet alakítani, így az adat-hozzáférési korlátozások érvényesítése megoldható a meglévő alkalmazások bármilyen módosítása nélkül.

ORACLE DATABASE VAULT**KAPCSOLÓDÓ TERMÉKEK:**

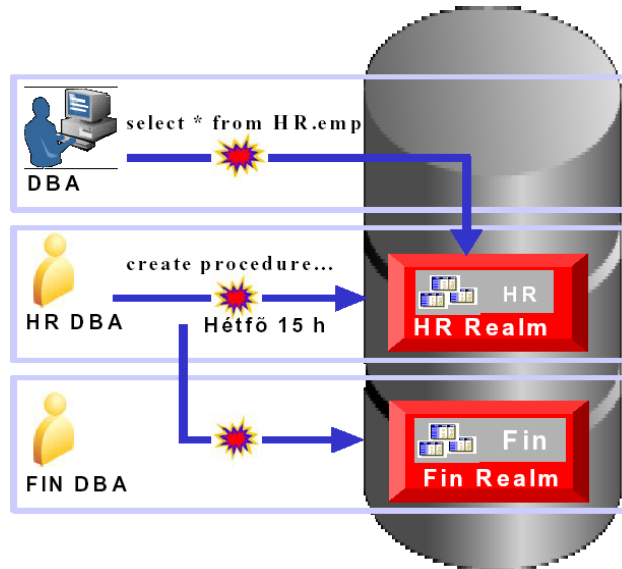
Az alábbi szoftverek segítenek a biztonság további erősítésében, és ezzel a biztonsági, személyes adatvédelmi és jogszabályi követelmények teljesítésében:

- Oracle Database 10g Release 2 – Oracle Label Security
 - Többszintű biztonság
 - Az érzékeny adatok védelme
 - Felhasználói biztonsági jogosítványok kezelése
 - Együttműködés az Oracle Identity Management személyazonosság-kezelő funkcióival
 - Common Criteria szabvány szerinti EAL4-es szint
- Oracle Database 10g Release 2 – Oracle Advanced Security
 - Transzparens adattitkosítás az alkalmazás meglévő SQL-kódjának módosítása nélkül
 - Erős hitelesítés
 - Hálózati adattitkosítás
- Oracle Secure Backup
 - A szalagra mentett adatok védelme
 - Az Oracle Home és az Oracle Alkalmazások adatainak biztonsági mentése, fájlrendszer támogatása
 - Együttműködés az Oracle Recovery Managerrel (RMAN), AES titkosítás 256 bitig
 - Interfész az Enterprise Managerhez a könnyű kezelhetőség érdekében

Az alkalmazások adatainak védelme a DBA és az erős jogosultságokkal rendelkező felhasználók illetéktelen beavatkozásától

Mérvadó biztonsági felmérések azt mutatták ki, hogy az esetek több mint 70%-ában az információs rendszerek ellen intézett támadások és az adatvesztés hátterében „belső emberek” álltak, akik a rendszerhez és az adatokhoz valamilyen szintű jogosult hozzáféréssel rendelkeztek. Az Oracle Database Vault segítségével megakadályozható, hogy az adatbázis-adminisztrátor jogosultságait használva lássa az alkalmazások adatait. Egyszerűen egy tartományt kell csak kijelölni a védendő sémák és objektumok köré.

Ha egyszer egy tartomány (realm) és a kapcsolódó szabályok meghatározása megtörtént, a DBA továbbra is képes az adatbázis felügyeletére, de már nem láthatja, vagy nem változtathatja meg az alkalmazások adatait.



1. ábra: Az Oracle Database 10g Release 2 Database Vault kiegészítéssel

Az alkalmazásokhoz való hozzáférés szabályozása

Az Oracle Database Vault szabályai és tényezői segítségével lényegesen megszigorítható az alkalmazások biztonsága. Korlátozni lehet, hogy ki, mikor és honnan érheti el az alkalmazásokat. Mindezen funkciókat rugalmasan, az adott vállalati igényekhez alkalmazkodva lehet alakítani, így az adat-hozzáférési korlátozások érvényesítése megoldható a meglévő alkalmazások bármilyen módosítása nélkül. A napszak, az adatbázis kliens helye a hálózaton belül vagy az egyedileg meghatározott más jellemzők mind olyan tényezők lehetnek, amelyeket egyenként vagy kombinálva több tényező hitelesítés megvalósítására lehet felhasználni, és szabályozható velük az alkalmazáshoz való hozzáférés. Az adatbázishoz való hozzáférés például egy meghatározott köztesrétegre vagy az adatbázis-kiszolgálón futó kötegelt feldolgozásokra korlátozható. A Database Vaultra épülő többtényezős hitelesítés jelentősen megszilárdítja a biztonságot.

Az adatbázisok védelme a nemkívánatos módosításoktól

Az Oracle Database Vault a felelősségi körök szétválasztásán alapuló hatékony biztonsági szabályokat tesz lehetővé, és védi az adatbázist a jogosulatlan módosításoktól. Megakadályozza, hogy egy CREATE USER jogosultsággal rendelkező DBA új felhasználót hozzon létre, ha nincs meg a megfelelő felhasználó-adminisztrátori szerepköre. Ezen túlmenően parancs szintű szabályokat lehet meghatározni mindegyik SQL-parancshoz, amelyekkel ellenőrizhető annak végrehajtása.

Adminisztrátori felület és kimutatáskészítés

Az Oracle Database Vault adminisztrátori felülettel és előre definiált biztonsági kimutatásokkal rendelkezik. A biztonsági adminisztrátor számára így áttekinthetővé válnak a biztonsággal kapcsolatos események, és megfelelően védheti az adatbázist és az alkalmazásokat.