

ORACLE ADVANCED SECURITY

FŐ JELLEMZŐK ÉS ELŐNYÖK



ORACLE ADVANCED SECURITY

- Elősegíti a hatósági előírások betartását
- Transzparens adattitkosítás (Transparent Data Encryption)
- Könnyen konfigurálható hálózati titkosítás és adatintegritás
- A meglévő biztonsági keretrendszer hasznosítása az erős hitelesítéshez: Kerberos, nyilvános kulcsú infrastruktúra (PKI), RADIUS
- A kliensek és/vagy szerverek kulcsainak chipkártyás védelme
- Adatok fokozott védeleme és azok bizalmas jellegének megőrzése a szervezet informatikai rendszereiben

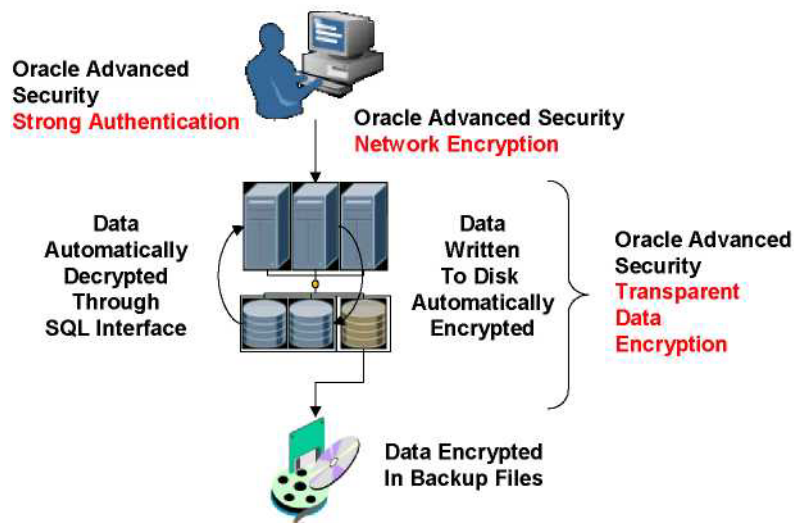
Az Oracle Advanced Security hatékony technológiákkal segíti elő a hatósági és belső előírások érvényesítését. Az érzékeny adatokat az adatbázison belül és a hálózaton való áthaladásukkor egyaránt védi az egységes biztonsági szolgáltatásként megjelenő kombinált hálózati titkosítással és transzparens adattitkosítással. Ezáltal gondoskodik az adatok biztonságáról akár az adathordozó eltulajdonítása, akár a hálózaton bekövetkező adattagadás, adatisméltés, lehallgatás vagy módosítás esetén. Az Oracle Advanced Security az Oracle adatbázisokkal folytatott teljes kommunikációt képes titkosítani. A megoldás transzparens adattitkosítási funkciója nagyban leegyszerűsíti a titkosítás alkalmazását az adatbázison belül. Az érzékeny adatok egyetlen paranccsal titkosíthatók az adatbázisban. Emellett az Oracle Advanced Security erős hitelesítéssel ellenőrzi az adatbázis-felhasználókat, így az alkalmazások felhasználói PKI, Kerberos vagy RADIUS segítségével igazolhatják személyazonosságukat.

Az érzékeny adatok automatikus titkosítása

A legtöbb titkosítási megoldáshoz az alkalmazás programkódjából kell speciális titkosító függvényeket meghívni. Ez idő- és pénzigényes, hiszen jellemzően jól kell ismerni hozzá az alkalmazást, ráadásul programkód írását, illetve módosítását igényli. A legtöbb szervezetnek általában nincs ideje vagy kellő szakértelme ahhoz, hogy a meglévő alkalmazásokat módosítsa a titkosító rutinok meghívásához. Emellett a már működő rendszerek utólagos kiegészítése titkosítással manuális feladat, ami számos hibalehetőséget hordoz. A titkosítási rutinhívásokat kézzel kell beilleszteni a program megfelelő helyeire. Az Oracle Advanced Security transzparens adattitkosítása megoldja ezt a problémát, mivel a titkosító mechanizmus mélyen az Oracle adatbázis-kezelőbe van beágyazva. Egy alkalmazás érzékeny adatainak titkosításához elegendő egyetlen „alter table” utasítás, amelyet az adatbázis-adminisztrátor is végrehajthat:

```
SQL>Alter table credit_rating modify(person_id encrypt no salt)
```

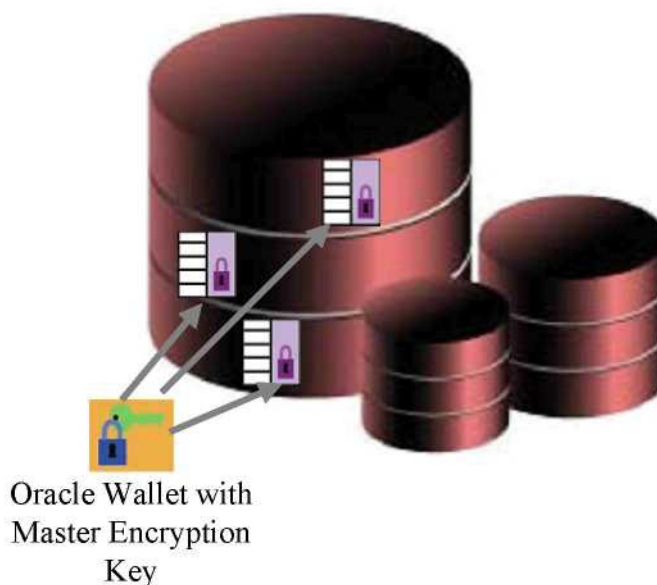
Az SQL-ben megírt alkalmazási logika minden módosítás nélkül zavartalanul működik tovább a titkosított adatokkal. Más szóval az alkalmazásokban nem módosul az a programkód, amely az adatoknak az adatbázistáblába való beillesztését végzi, az adatokat az Oracle adatbázis-kezelő titkosítja automatikusan a lemeze kiírás előtt. A meglévő biztonsági mentési programok ugyanúgy használhatók tovább, de most már a szalagra mentett adatok is titkosítva vannak. A későbbi Select műveletek szintén transzparensen visszafejtik az adatokat az alkalmazás működésének bármilyen megzavarása nélkül. Ez azért fontos, mert a meglévő alkalmazások arra vannak felkészítve, hogy titkosítatlan adatokat lássanak.



A titkosító kulcs beállítása

Az Oracle transzparens adattitkosítása biztosítja a titkosítás működéséhez szükséges kulcskezelő infrastruktúrát. A titkosítás úgy működik, hogy a titkosító rutin megkapja a tiszta szöveges formátumú adatot, és emellé egy titkos kulcsot is kap. A kulccsal titkosítja a tiszta szöveges adatot, és visszaadja a titkosított adatot. A kulcsok létrehozása és karbantartása korábban jellemzően az alkalmazás feladata volt. A transzparens adattitkosítás viszont önállóan gondoskodik egy az egész adatbázisra érvényes főkulcs (master key) generálásáról és karbantartásáról. Az adatbázis főkulcsának szerepe az, hogy ezzel titkosítják az Oracle adatbázis-kezelő által az egyes táblákhoz automatikusan létrehozott saját titkosító kulcsokat. A főkulcs nélkül az Oracle adatbázis semmilyen adatát nem lehet visszafejteni. Az Oracle adatbázis elindításakor az adatbázis-adminisztrátor (DBA) egy megfelelő jelszóval megnyit egy Oracle Wallet nevű objektumot. Ez a „pénztárca” tartalmazza a főkulcsot, és mindenképpen meg kell nyitni bármilyen titkosított adat elérése előtt. A „pénztárca” jelszava külön jelszó, amely eltérhet a rendszer vagy a DBA jelszavától. Nagyobb szervezeteknél egy külön biztonsági DBA feladatkörébe tartozhat, a „pénztárca” megnyitása. Mielőtt az adatbázisban első ízben alkalmaznák a titkosítást, inicializálni kell az adatbázis főkulcsát.

```
SQL> alter system set encryption key identified by "lwq!r23t";
```



A transzparens adattitkosítás által támogatott adattípusok

A transzparens adattitkosítás első változata az alábbi adattípusokat támogatja. A később megjelenő változatok további adattípusokat is támogatnak majd.

Adattípus	A transzparens adattitkosítás támogatja
varchar2	Igen
nvarchar2	Igen
number	Igen
date	Igen
binary float	Igen
binary double	Igen
timestamp	Igen
raw	Igen
char	Igen
nchar	Igen

Teljesítmény

A szokásos titkosítási módszerek gondot okoznak az alkalmazások adattábláinak meglévő indexei esetében, mivel az indexadatok nem kerülnek titkosításra. A transzparens adattitkosítás viszont a táblához tartozó indexértékeket is titkosítja. Ez azzal az előnnyel jár, hogy az alkalmazáson belüli egyezőségkeresések teljesítménye gyakorlatilag nem csökken. Tegyük fel például, hogy egy alkalmazás egy CREDIT_RATING nevű hitelbesorolási táblát tartalmaz, amelyben a személyre utaló PERSON_ID oszlopot titkosítani kell.

```
SQL>Connect appowner
```

```
SQL>Alter table credit_rating modify(person_id encrypt no salt)
```

```
SQL>Create index person_id_idx on credit_rating (PERSON_ID)
```

```
SQL>Select score from credit_rating where PERSON_ID = '235901';
```

A példa esetében a PERSON_ID értékek mind az alaptáblában, mind az indexben titkosításra kerülnek. Az Oracle adatbázis az új indexet fogja használni akkor is, ha a PERSON_ID érték az indexben titkosítva van.

Kulcskezelő keretrendszer

Az Oracle Advanced Security transzparens adattitkosítása integráltan együttműködik az Oracle „wallet” szolgáltatásával, és gondoskodik a titkosítási főkulcs (master key) kezeléséről. Ez lehetővé teszi a titkosítási főkulcsok módosítását, így a titkosított szalagos mentések visszafejthetők az Oracle adatbázisba való későbbi visszatöltésükkor.

Transzparens adattitkosító algoritmusok

A transzparens adattitkosítás 256 bites kulcsméretig támogatja a 3DES és Advanced Encryption Standard (AES) titkosító algoritmusokat.

Az érzékeny adatok védelme a hálózaton

Az Oracle Advanced Security az Oracle adatbázisok felé irányuló és a kifelé menő forgalmat egyaránt védi. A felhasználók a hálózaton áthaladó adatok védelméhez választhatnak az Oracle Advanced Security natív titkosító és adatintegritási algoritmusai, illetve az SSL közül. Néhány tipikus helyzet, amely hálózati szintű titkosítást igényel:

- Az adatbázisszerver tűzfal mögött működik, és a felhasználók kliens–szerver alkalmazásokkal érik el a szervert
- A DMZ-ben működő alkalmazás-szerver és a második tűzfal mögötti adatbázis-kezelő közti kommunikációt titkosítani kell
- Az adatbázisok közti adatforgalmat titkosítani kell

Az Oracle Advanced Security natív titkosító és adatintegritási algoritmusai nem igénylik PKI kulcskezelő infrastruktúra létesítését. Az adatbázis-kezelő későbbiekben megjelenő verzióiban sorra megtalálhatók lesznek az elfogadott újabb titkosító algoritmusok. A legújabb ilyen algoritmus az Advanced Encryption Standard (AES), amely a DES-hez képest jobb biztonságot és teljesítményt nyújt. A jelenleg támogatott titkosító és adatintegritási algoritmusok teljes köre:

- AES (128, 192 és 256 Key)
- RC4 (40, 56, 128, 256 Key)
- 3DES (2 Key és 3 Key)
- MD5
- SHA1

Az SSL alapú titkosítást a PKI infrastruktúrát alkalmazó szervezetek használhatják. A TLS 1.0 támogatása az Oracle Database 10g Release 1 változatában jelent meg. Az Oracle Advanced Security az Oracle Database 10g Release 1 változatában megjelenő TLS 1.0 protokollhoz biztosított először AES kódolási készletet („cipher suite”).

Könnyű konfigurálás, nem igényli az alkalmazások módosítását

A hálózati titkosításhoz és adatintegritás-védelemhez – az Advanced Security opció kliens és szerver gépeken történő telepítését követően – elegendő a szerver és/vagy a kliens hálózati beállításait módosítani. Ezért a legtöbb szervezet könnyen be tudja vezetni, mivel az alkalmazásokat nem kell módosítani.

Erős hitelesítési szolgáltatások

Az információkhoz való illetéktelen hozzáférés az idők kezdete óta komoly gondokat okoz. Korunkban már számos üzleti döntés alapul sok terabájtnyi adat átbányászása során kigyűjtött információkon. Az érzékeny információk védelme nélkülözhetetlen a versenyképesség megőrzéséhez. Ezért a fontos adatokat tároló olyan rendszerekhez való hozzáférés, mint az Oracle Database 10g, csakis a felhasználók megfelelő azonosításával és hitelesítésével történhet. A felhasználó azonosságának ellenőrzéséhez nem elegendő a szokásos felhasználói név és jelszó.

Az Oracle Advanced Security lehetőséget kínál a szervezet meglévő biztonsági infrastruktúrájának (Kerberos, PKI, RADIUS) hasznosítására az erős hitelesítéshez.

A PKI-támogatás részeként képes ellenőrizni az X.509v3 szerinti tanúsítvány-visszavonást a fájlrendszerben tárolt visszavont tanúsítványok listáján (Certificate Revocation Lists), az Oracle Internet Directory címtáron vagy a CRL disztribúciós pontokon keresztül. Emellett az Oracle adatbázis-kezelők, valamint a kliensek/felhasználók chipkártyán, vagy a PKCS 11 ipari szabványnak megfelelő más hardveres tárolómodulokon tárolt PKI-igazolóadatokkal is hitelesíthetik magukat. Ez különösen előnyös megoldás, hiszen így a felhasználók szabadon mozogva több helyről is elérhetik az adatbázist kliens–szerver alapú, vagy webes alkalmazásokon keresztül. A szerreléréshez szükséges igazoló adatok hardvereszközös tárolása emellett olyan fokozott biztonságot nyújt, amely egyes esetekben alapvető elvárás.

Együttműködő ipari szabványok

Az Oracle Advanced Security SSL-kliense bármely ipari szabványú PKI-infrastruktúrában alkalmazható. Például a Verisign, a Thawte, az RSA Keon és az Oracle Certificate Authority tanúsítványszolgáltatók által kibocsátott tanúsítványok alkalmasak az Oracle Database 10g Release 2 változatához, mivel ezek a szolgáltatók elfogadják a szabványos PKCS7 szerinti tanúsítványkérelmeket, és az X509v3-nak megfelelő tanúsítványokat bocsátanak ki. Az Oracle Advanced Security külön Entrust adaptert is biztosít, amellyel az üzleti alkalmazások az Entrust PKI-jét is használhatják az Oracle Database 10g Release 2 változatával.

Az Oracle Advanced Security egy Kerberos-kliens is tartalmaz, amellyel a Kerberos biztonsági keretrendszer integrálható az Oracle Database 10g Release 2 változatával. A Kerberos-kliens konfigurálása után a felhasználók az MIT v5 előírásainak megfelelő Kerberos-kiszolgálók vagy Microsoft KDC kiszolgálók által kibocsátott Kerberos v5 jegyekkel jelentkezhetnek be az Oracle adatbázisba. Így az ügyfelek az Oracle Advanced Security Kerberos alapú megoldásával tovább használhatják heterogén környezetüket.

Az Oracle Advanced Security RADIUS-kliens is tartalmaz, amely lehetővé teszi, hogy az Oracle Database 10g Release 2 változata elfogadja a RADIUS-kiszolgálók által megerősített hitelesítéseket és jogosítványokat. Ez különösen azoknál a szervezeteknél hasznos, amelyek kétszintű hitelesítést igényelnek, ahol a felhasználó azonosságát egyrészt olyasmivel igazolja, amit csak ő tud (jelszó vagy PIN-kód), másrészt pedig olyasmivel, ami csak az ő birtokában van (tokenkártya). Több gyártó is kínál ilyen tokenkártyás rendszereket.

KAPCSOLÓDÓ TERMÉKEK

Az alábbi termékek és funkciók segítik még a szervezet biztonsági rendszerének megerősítését:

- Oracle Database 10g–Oracle Label Security: címke alapú sor szintű hozzáférés szabályozás
- Virtual Private Database: egyedi sor szintű biztonsági beállításokra épülő „virtuálisan privát adatbázisok”
- Global Application Context: biztonságfelügyelet
- Fine Grained Auditing: kontextus alapú biztonsági auditálás
- Enterprise User Security: az adatbázis-felhasználók felügyelete az Oracle Identity Management keretrendszerben
- Secure Application Roles: az adatbázis-objektumok hozzáférési jogosultságainak policy alapú szabályozása
- Hatékony proxyszolgáltatások a többretegű alkalmazási modellekhez

A jövőbeni fejlesztések iránya

Az Oracle a hardveres biztonsági eszközök gyártóival együttműködve arra törekszik, hogy az Oracle Advanced Security adattitkosítási főkulcsát hardveres biztonsági eszközbe beépítve lehessen használni. Emellett az Oracle azon dolgozik, hogy a transzparens adattitkosítást az oszlopok szintjén túl kiterjessze teljes objektumokra, például egész táblákra, táblaterekre és partíciókra. Végül pedig egy újabb hitelesítési szint fog bekerülni a termékbe, amely még szigorúbban korlátozza az adatok visszafejtéséhez használt kulcsokhoz való hozzáférést, így az objektum szinten túlmenő további hozzáférés-korlátozást biztosít. Az ipari szabvánnyá váló újabb titkosító algoritmusok is megjelennek majd a termék újabb verzióiban.

Elérhetőség

Az Oracle Advanced Security az Oracle Database 10g Release 2 változatának Enterprise Edition kiadásával licencelhető. Az Oracle Database 10g 2 Enterprise Edition által támogatott összes platformon elérhető. A külső cégek hitelesítési szolgáltatásainak azonban nem mindegyike érhető el minden támogatott platformon. A termék elérhetőségét adott platformokon a helyi Oracle-képvisellel lehet tisztázni.