Oracle Access Observer

Bevezető

- Egy Oracle-alapú felhasználói rendszer adatbázis-tábláihoz való hozzáférés nyilvánvalóan az Oracle objektum-privilégiumainak beállításán múlik. Szerencsés esetben ezekhez a táblákhoz csak a felhasználói programokon keresztül férnek hozzá, az adat-manipulációk csak és kizárólag ezeknek a programoknak a segítségével történik.

- Aggályosnak tekinthető, ha ezeken a táblákon, egyéb segédprogramok segítségével adatokat módosítanak, visznek fel, törölnek, adatokat listáznak ki. Egy ilyen eseményt a továbbiakban incidensnek fogunk nevezni.

Ismertető

A Montauk Access Observer képes arra, hogy riportban jelenítse meg azon Oracle-felhasználókat, akik illetéktelenül hajtanak végre select, insert, update vagy delete utasításokat a megfigyelés alá bevont táblákon

Esettanulmány

Egy szoftverfejlesztő cég Oracle-bázisú felhasználói rendszert szállít le egy megrendelőjének. A rendszer tábláit, tárolt eljárásait, és egyéb objektumait egy schema tartalmazza.

A szoftverfejlesztő cég célja, hogy egy adott „white list” tagjain túl, -- beleértve a megrendelő erős usereit is (például adminisztrátorokat) -- mások ne manipulálják, ne nézegessék a táblákat. A fejlesztő cég a Montauk Access Observer segítségével folyamatosan képes informálódni arról, hogy rendszerének tábláit, ki, mikor, mivel manipulálta, nézegette, olyan programok segítségével, amelyek nem képezik a felhasználói rendszer részét.

Esettanulmány

A hozzáférés megtagadása itt nem jöhet szóba, viszont a háttérben működő Montauk Access Observer képes riportot adni az incidensekről, azokról az eseményekről, amikor a „white list”-en kívüli felhasználók fértek hozzá a megfigyelés alá bevont táblákhoz.

Technikai ismertető

Szofi Algorithmic Research Kft

MNTK_DICT

	DICT_KEY	DICT_VALUE
1	sysConst/liveLimit	30
2	sysConst/licenceOwner	AdviseSorft
3	sysConst/copyRight	Szofi Algorithmic Research Inc.
4	sysConst/schemaName	IDIOSI

A rendszer szótára a szokásos dictionary. A rendszer működését vezérlő paramétereket tartalmazza.

A **sysConst/liveLimi**t kulcshoz tartozó érték (a képen 30) azon napok számát jelenti, amikor egy incidens elavulttá válik.

A **sysConst/schemaName** annak a séma usernek a nevét (esetünkben: IDIOSI) tartalmazza, amelynek a tábláit megfigyelés alá helyezzük.

MNTK_WHITE_LIST

	SCHEMA_ID	SCHEMA_NAME
1	113	SIEBEL
2	110	SCOTT

Azon felhasználói sémák, amelyek hozzáférése a megfigyelés alá bevont táblákhoz nem jelent incidenst. Ezek a példában SIEBEL és SCOTT.

Megfordítva: minden olyan felhasználó, amely nem eleme ennek a listának, az ugyan hozzáférhet a megfigyelés alá vont táblákhoz, de ez az esemény incidensként definiált.

MNTK_OBSERVER package

```
Connected to Oracle Database 12c Enterprise Edition Release 12.1.0.2.0
Connected as idiosi


SQL> execute mntk_observer.start_diagnostic;

PL/SQL procedure successfully completed

SQL>
```

A package eljárásai tartalmazzák azt az üzleti logikát, amely az incidens-detektálást végzi.

A start_diagnostic metódus indítása lehet alkalomszerű, a riport generálása előtt, de ütemezhető is.

MNTK_REPORT_INCIDENT

	NAME_OF_RUNNER_SCH	ID_OF_R	RUNNING_TIME	NAME_OF_REFERRED_TABLE	PROGRAM	MACHINE
1	HOMERSIMPSON	143	2017.11.30. 10:39:43	TABLE_MINTA1	plsqldev.exe	WORKGROUP\KFKI
2	HOMERSIMPSON	143	2017.11.30. 10:38:58	TABLE_MINTA2	plsqldev.exe	WORKGROUP\KFKI
3	HOMERSIMPSON	143	2017.11.29. 14:18:05	TABLE_MINTA3	plsqldev.exe	WORKGROUP\KFKI
4	HOMERSIMPSON	143	2017.11.29. 12:07:20	TABLE_MINT2	plsqldev.exe	WORKGROUP\KFKI
5	BART	143	2017.11.29. 14:18:36	TABLE_MINTA1	plsqldev.exe	WORKGROUP\KFKI
6	BART	143	2017.11.29. 14:18:46	TABLE_MINTA4	plsqldev.exe	WORKGROUP\KFKI

A fenti virtuális tábla jeleníti meg az incidenseket. A képen az attribútumoknak csak egy részlete látható. A kérdéses SQL-mondat mellett a diagnosztika leíró paramétereit is megjelenítjük.

A fenti riport úgy értelmezhető, hogy egy HOMERSIMPSON és egy BART nevű user a jelzett időpontokban SQL utasítást adott ki IDIOSI felhasználó adott nevű tábláira, az adott programmal, az adott gépről. (A többi attribútum a listán nem látható.)

További információk:
+36 30 209 0658
http://szofiusa.com/callcenter_hu.html