Enterprise User Security

Adatbázis felhasználók
központosított, címtár alapú kezelése

Lakatos István / IT üzemeltetés

Allianz

Allianz

Mi is hiányzik nekünk?

Admin-felhasználó:

1. „Kérek egy usert olyan jogokkal mint ahogy az alkalmazás fut”

   Admin válasz: Elküldöm az alkalmazás jelszót, azzal be tudsz lépni

2. „Készíts egy olyan usert ami mostani és a később létrehozandó táblákra és olvasási joggal bír”

   Admin válasz: Ez nem kivitelezhető, fordulj az alkalmazás fejlesztőjéhez, hogy tartsa karban a megfelelő jogosultságokat.

3. Kérem oldjátok meg, hogy minden adatbázisban mindig ugyanaz legyen a jelszavam”

   Admin válasz: ?????

4. „Az élesben nem kérek hozzáférést, de minden másolásnál hozzatok létre egy olvasási joggal bíró usert a számomra”

   Admin válasz: Akkor most megint programokat írunk?

Mi is hiányzik nekünk?

Vezetői problémák:

1. „Kérem adjátok meg, hogy a kiemelt jogosultságok mikor kerültek igénylésre, ki hagyta jóvá, meddig érvényes stb…!”

2. „Állítsatok be olyan szabályokat, hogy kampány alatt csak néhány kiemelt felhasználó tudjon az adatbázisba belépni, üzletileg érzékeny adatokat tartalmaz”

3. „Incidens elhárítás miatt a másolati adatbázisra csak 36 órára engedjétek be a felhasználót.”

Kísérletek a probléma megoldására

1. Csak igények alapján dolgozunk, majd az igényekről nyilvántartást vezetünk, rengeteg adminisztrációs teher keletkezik.

2. Közös használatú felhasználók bevezetése, majd a jelszavak naponta történő módosítása, és a jelszó publikációra egy külön alkalmazás használata.

3. Megelőző behatolás védelem fejlesztése a közös felhasználókra, megfelelő adatbázis triggerek használatával. A jogosultsági szabályok tárolása adatbázisonként eltérő lehet.

- Egyszerűsített admisztrációs tevékenységet.
- IDM vezérelt igénylés folyamatokat
- Nagyobb átláthatóságot és a kiemelt jogosultságok naprakészen tartását
- A meglévő elemekből történő építkezést
- Gyors bevezetést
- A felhasználók ne tehernek érezzék az új rendszer használatát.

Mit is várunk ez EUS bevezetésétől?

Az építkezéshez szükséges elemek

- Oracle Unified Directory (11.1.2.1.0) (ldap replikációval)
- Egy Websphere application szerver az Unified Directory kezelésére
- A meglévő IDM rendszerben egy olyan struktúra kialakítása ahol az adatbázisokat a felhasználói és az alkalmazás usereket tárolni lehet.
- Az IDM-ben az igénylési folyamatok kiterjesztése az adatbázis hozzáférésre.

A rendszer egyszerűsített működése:

- Egyes adatbázis usereknél be kell állítani a külső (proxy) authenikáció lehetőségét.
- Az adatbázisokat meg kell tanítani, hogy az azonosításhoz, a jogosultságok lékéréséhez az információkat hol találják, honnan kell elérni (OUD)
- Az OUD tárolja részletesen, hogy az egyes adatbázisokban a természetes userek milyen más userek nevébe léphetnek be
- Az OUD jogosultság karbantartása az IDM segítségével történik

Implementációs lépések - IDM + OID	Elvégezve
Az IDM számára az adatbázisok megismertetése	✓
Az adatbázis felhasználók betöltése az IDM-be	✓
Az OUD-ban az Enterprise domainek létrehozása	✓
Enterprise User-ek létrehozása az OUD directory tree-ben	✓
Enterprise Domainek-en értelmezett User-Schema Mapping létrehozása az Enterprise User-ek és eus Global Database User és közötti leképezés megvalósításához	✓
A password reset alkalmazás felkészítése az új OUD kezelésére	✓
Az ősfeltöltés a meglévő információk, jogosultságok alapján	✓

Implementációs lépések - Adatbázis oldalon	Elvégezve
ldap.ora konfigurációs fájlban az OUD példányok elérhetőségének megadása.	✓
sqlnet.ora módosítása az OUD alapú TNS névfeloldás támogatása érdekében. ... NAMES.DIRECTORY_PATH= (LDAP,...	✓
DB_UNIQUE_NAME paraméter beállítása.	✓
Wallet location szükség szerinti helyes beállítása az *sqlnet.ora fájlban* (WALLET_OVERRIDE és WALLET_LOCATION változók)	✓
Adatbázis Oracle Contextbe regisztrációja a dbca silent módú futtatása segítségével.	✓
ldap_directory_access indítási paraméter ellenőrzése. Kívánt érték: PASSWORD	✓

Implementációs lépések - Adatbázis oldalon	Elvégezve
Global Database User létrehozása a következő módon: *create user eus identified globally;* *grant connect to eus;*	✓
Megfelelő sémák (pl. alkalmazás sémák, lekérdező sémák) proxyzhatóvá tétele.	✓
Proxy User jelszóváltoztatásának megakadályozása	✓
Új adatbázis létrehozása esetén az adatbázis regisztrációja	✓
A klónozó eljárások felkészítése a proxy userek kezelésére	✓

A eredmény:

1. Felhasználók annyit éreznek, hogy
   connect usernév/jelszó
   helyett használandó:
   connect usernév/jelszó [proxy user]

2. A felhasználók minden adatbázisba ugyanazzal a usernév jelszó párossal tudnak belépni.

3. A jogosultság igénylése egyszerűsített és önkiszolgáló módon az IDM rendszerben történhet.

4. A jogosultságok rendszere átlátható, rendszeresen ellenőrizhető felülvizsgálható

5. Az adatbázis adminisztrátornak csak abban az esetben kell tevékenykednie, ha új adatbázis keletkezik, vagy új alkalmazás érkezik.