

Az Oracle COREid bemutatása

*Az Oracle tájékoztatója,
2005. május*

BEVEZETÉS

A hatósági előírások és törvényi szabályozás fokozottabb betartása, a működési költségek csökkentése, valamint az alkalmazások jobb elérhetősége érdekében a nagy szervezetek egyre elterjedtebben alkalmazzák a különböző identitáskezelési megoldásokat. A szilárd identitáskezelési háttérhez olyan integrált technológiára van szükség, amely biztosítja a felhasználói adatok teljes életciklusra kiterjedő kezelését, a profiladatok biztonságos tárolását és az ezeken a profilokon alapuló kiterjedt hozzáférés-szabályozást.

Az Oblix felvásárlásával és az Oblix termékválasztékának az Oracle Application Server alkalmazáskiszolgálóba történő integrálásával az Oracle a fenti alkalmazási területek mindegyikéhez átfogó megoldást kínál. Az Oracle COREid rendszerbe állítása a világ első ezer legnagyobb cége közül soknál éppen most van folyamatban, és már ma is a COREid működteti a világ számos nagy portálját. A COREid a vállalatok számára biztonságot, adminisztratív felügyeletet és a többféle szoftvergyártó termékein és platformjain futó portálok, extranetek és intranetek nagyobb átláthatóságát biztosítja.

Ez a tanulmány az Oracle COREid fő összetevőiről és funkcióiról ad tájékoztatást. A COREid termékcsalád két terméket tartalmaz, ezek a COREid Access and Identity és a COREid Provisioning.

COREID ACCESS AND IDENTITY

A COREid Access and Identity már 1996 óta kapható, és kritikus fontosságú szolgáltatásokat kínál a hozzáférés-szabályozás, az egyszeri bejelentkezéses hitelesítés és a felhasználói profilok kezelése terén. A szoftver emellett a fenti funkciókra kiterjedő és azok összefüggéseire rávilágító auditálási kimutatásokat is biztosít.

A hozzáférési jogosultságok kezelése és az egyszeri bejelentkezés (SSO) tekintetében a COREid Access and Identity kulcsfontosságú funkciókat tartalmaz a hozzáférési szabályok létrehozásához, karbantartásához és érvényesítéséhez.

Access Manager

A COREid Access Manager egy olyan grafikus eszköz, amely a hozzáférési szabályok létrehozására és kezelésére, valamint az erőforrások védelmének beállítására szolgál, és a szabályok helyes működésének ellenőrzése érdekében képes szimulált felhasználói hozzáféréssel tesztelni azokat.

Access Server

A COREid Access Server olyan külön szoftveres kiszolgáló, amely önállóan vagy fürtözött (terheléskiegyenlítési vagy hibátűrő redundáns) konfigurációban telepíthető, és webes, illetve nem webes erőforrások esetében egyaránt képes a hozzáférési szabályok érvényesítésére. Az Access Server dinamikus szabályértékelést végez, amikor a felhasználók a webszolgáltatásokat használják. Ugyanakkor hitelesítési, jogosultság-hozzárendelési és auditálási szolgáltatásokat is kínál.

Hitelesítési beépülő modulok

A COREid Access beépülő modulok (pluginek) fejlesztését szolgáló alkalmazói programinterfészt (API) kínál a különböző hitelesítési módszerek és eszközök integrálásához. A termék gyárilag támogatja a chipkártyák, mint például a SecurID használatát. A plugineket támogató API-val az ügyfelek olyannyira kibővíthetik a COREid felhasználását, hogy az szinte bármilyen hitelesítési formával képes együttműködni, köztük a biometrikus és a kéttényezős azonosítással is.

Az identitásfelügyelet szempontjából a COREid Access and Identity kulcsfontosságú funkciókkal támogatja a címtár-adminisztrátorok munkáját. A nagy méretű portálokat vagy extraneteket üzemeltető ügyfeleknél, ahol több százezer vagy millió felhasználóról beszélünk, a szabványos felhasználóadminisztrációs eszközök gyakran nem bírják a nagy terhelést. A felhasználói adattárak felfelé méretezésének egyetlen módja (LDAP vagy relációs adatbázis alapú címtáraknál egyaránt) olyan speciális szolgáltatások bevezetése, mint a delegált rendszeradminisztráció, a dinamikus csoportfelügyelet, illetve az önkiszolgáló felhasználói adminisztrációs és regisztrációs szolgáltatások.

Leosztható adminisztráció

Amikor a felhasználói címtár több ezer vagy több millió felhasználót tartalmaz, akkor képtelenség, hogy egyetlen adminisztrációs csoport felügyelje a folyamatosan történő profilváltozásokat. Az ilyen méretű adatbázisokkal dolgozó vállalatoknak több tucat címtár-adminisztrátorra lenne szükségük, hogy lépést tartsanak a terhelésnövekedéssel. A feladat sokkal jobban megoldható a leosztható adminisztráció módszerével, ahol a felhasználói csoportok felügyelete az adott csoportok adminisztrátorainak felelősségi körébe tartozik. Ha például egy gyártó cég több ezer beszállító részére egy beszállítói portált üzemeltet, akkor a beszállító vállalatokhoz tartozó felhasználókért az adott beszállító rendszergazdája felel. Ennek eredménye a munkateher megosztása, a pontosabb adatnyilvántartás és a méretezhető rendszeradminisztráció.

A piacon jelen lévő hasonló termékek közül a COREid Access and Identity rendelkezik a legrugalmasabb és legjobban méretezhető leosztható adminisztrációs funkciókkal, amelyeket már ma is a világ legnagyobb portáljai alkalmaznak. A COREid leosztott adminisztrációs funkciói olyan megbízhatóan működnek, hogy számos olyan Oracle-ügyfél, amely már megvásárolta valamelyik konkurens hozzáférés-szabályozási megoldást, úgy döntött, hogy fölé telepíti a COREid-t, csak hogy kihasználhassa az Oracle szoftverének leosztott felügyeleti képességeit.

Dinamikus csoportkezelés

Nagyon hasznos és gyakori identitáskezelési funkció a felhasználók csoportokhoz rendelése, amellyel finomabb hozzáférés-szabályozás és használatelemzés érhető el. Nagy számú felhasználó esetében azonban a statikus csoportokhoz rendelés nem túl jól működik. Ennél jobb módszert kínálnak a felhasználói attribútumok alapján létrehozott dinamikus csoportok. Például egy vezeték nélküli telefonszolgáltató ügyfélszolgálati portáljához több millió felhasználó tartozhat, akik közül az egyik dinamikus csoport az „SMS-felhasználók” lehet, ahová azokat a felhasználókat sorolja be a rendszer, akiknek a bejelentkezéséhez az SMS-üzenetküldés aktíválva van. A csoporthoz tartozó felhasználóknak így automatikus hozzáférést lehet biztosítani a további segítséget nyújtó webhelyekhez. Mivel az ügyfelek ezt a lehetőséget bármikor ki- és bekapcsolhatják, lehetetlen a felhasználókat manuálisan ehhez a csoporthoz rendelni. A COREid dinamikus csoportfunkcióival és a felhasználói profil attribútumait alapul véve a felhasználók automatikusan hozzáadhatók a csoporthoz vagy eltávolíthatók belőle. Amikor az ügyfél aktiválja az SMS-üzenetküldést, a címtárprofiljában aktiválódik egy állapotjelző, és a COREid azonnal hozzárendeli az ügyfelet az adott csoporthoz.

Önkiszolgáló felhasználói adminisztráció és regisztráció

Szintén növeli a rendszeradminisztráció méretezhetőségét, ha a felhasználóknak lehetővé tesszük, hogy profiljaikat saját maguk kezeljék. A szoftverben előre definiált önregisztrációs képernyők segítségével a felhasználók ügyintéző közreműködése nélkül vihetik fel adataikat a címtárba. Az önkiszolgáló regisztráció során a COREid munkafolyamatai gondoskodnak a szükséges ellenőrzésekről és a megfelelő eljárások követéséről, amikor a felhasználók felviszik profiljaikat. A COREid lehetővé teszi azt is, hogy a felhasználók az engedélyezett hozzáférési szinten belül megváltoztassák az attribútumaikat. Egyes felhasználók például frissíthetik a telefonszámaikat, de nem változtathatják meg a beosztásra vonatkozó megjelölést. Ezeknek a munkavállalóknak a felettesei jogosultak a beosztás megváltoztatására, de a fizetést ők sem módosíthatják stb. A COREid korlátlan hozzáférés-szabályozási rugalmasságot biztosít a felhasználói attribútumok területén, és munkafolyamatokat is rendel ezekhez a módosításokhoz. Ennek eredménye a nagyobb felhasználói kontroll és rugalmasság, miközben a rendszeradminisztráció szorosan szabályozott marad.

Nyomkövetési kimutatások

A nyomkövetési kimutatásokhoz a COREid Access and Identity egy kimutatási keretrendszer tartalmaz, így valamennyi biztonsági és profilkezelési eseményt egy központi relációs adatbázisban lehet naplózni. A belső és hatósági ellenőrzésekhez ma már részletesen tanúsítani kell a törvényi rendelkezéseknek és a belső előírásoknak történő megfelelést, és a rendszergazdák is szeretik kielemezni a biztonsági és azonosítási

műveleteket a hiányosságok kiszűréséhez. A leggyakoribb auditálási funkciókhoz előre definiált kimutatások állnak rendelkezésre, mint például:

- **Hitelesítési statisztikák** (a sikeres és a sikertelen hozzáférések aránya valamennyi COREid Access Serveren)
- **Jogosultság-hozzárendelési statisztikák** (az igényelt jogosultságok sikeres és a sikertelen megszerzésének aránya valamennyi COREid Access Serveren)
- **Sikertelenül igényelt jogosultságok** (felhasználónként)
- **Sikertelenül igényelt jogosultságok** (erőforrásonként)
- **Hozzáférés tesztelése**
- **Csoportelőzmények** (az összes módosítás valamennyi csoportprofilban)
- **Azonosítási előzmények** (felhasználónként)
- **Kizárt felhasználók**
- **Jelszó módosítások** (egy adott időtartamon belül)
- **Új, deaktivált, újra aktivált, ill. törölt felhasználók**
- **A felhasználói profilok módosítási előzményei** (valamennyi felhasználóra)
- **Deaktivált felhasználói csoportok**
- **Munkafolyamatok végrehajtási ideje**

COREID INTEGRÁCIÓS ÜGYNÖKALKALMAZÁSOK

A COREid Access and Identity számos integrációs ügynökalkalmazást is tartalmaz a többféle platformon futó alkalmazások felügyeletéhez és biztonságossá tételéhez. Ezen integrációs összetevők között valamennyi fontosabb webszerverhez, alkalmazáserverhez, illetve portálszerverhez megtalálhatók a többféle platformon futó előre definiált ügynökalkalmazások.

A COREid WebGates és AccessGates alkalmazások a harmadik féltől származó és a saját fejlesztésű infrastruktúratermékekbe beépülve elfogják a weben keresztül érkező kéréseket, és érvényesítik a COREid hozzáférési szabályrendszerét. A WebGates „előre gyártott” webkiszolgáló ügynökalkalmazásokat takar, míg az Access SDK lehetővé teszi, hogy az ügyfelek maguk hozzák létre AccessGates-szabályaikat az egyedi alkalmazásokra, ezzel kibővítve a COREid szabálykezelési és érvényesítési körét. Semmilyen más identitáskezelő szoftvergyártó nem nyújt ilyen széles körű szolgáltatást, amely különféle szoftververziókra, eltérő termékekre és operációs rendszerekre kiterjedő, átfogó védelmet nyújt a valós élet viszonyosságai között működő, éles környezetek számára.

COREID PROVISIONING

A COREid Provisioning automatikus funkciókkal segíti a felhasználók létrehozását, frissítését és törlését az olyan vállalati rendszerekben, mint például a címtárak, adatbázisok, levelezőrendszerek és ERP-rendszerek. Kulcsfontosságú funkciókat kínál a felhasználói adatok teljes életciklusra kiterjedő kezeléséhez, és szorosan együttműködik a COREid egyéb összetevőivel.

A vállalati rendszerekben a COREid kifinomult munkafolyamat-kezelést biztosít a felhasználók hozzáadásához, frissítéséhez és deaktiválásához. A felhasználói adatok automatikus kigyűjtésével és ellenőrzésével a vállalatok költségei csökkennek, lerövidül a rendszerek válaszáideje, és a szervezet jobban képes megfelelni a törvényi előírásoknak. A Fortune 500 vezető cégei közül már többen is használják a COREid Workflow szolgáltatásait, amelyek több tízezer felhasználó felügyeletét látják el.

A COREid Provisioningban a rendszerek jelszavainak szinkronizálására és a kapcsolódó módosításoknak a többi rendszerbe történő átvezetésére szolgál az Oracle Directory Integration and Provisioning (DIP) címtár-integrációs és -kezelő kiszolgálója. A DIP az olyan adattárak felhasználói bejelentkezéseinek felügyeletét szolgálja, mint például a relációs adatbázisok és az LDAP-címtárak, de ugyanezt biztosítja az olyan kereskedelmi alkalmazáscsomagokhoz is, mint az Oracle és a PeopleSoft HR.

ÖSSZEFOGLALÁS

A COREid Access and Identity, valamint a COREid Provisioning bevezetésével az Oracle a piacon elérhető legátfogóbb identitáskezelési megoldást kínálja, amely a felhasználói azonosító adatok teljes életciklusát lefedi a létrehozástól a használaton és a kimutatáskészítésen át egészen az adatok törléséig. Az Oracle Internet Directory és az Oracle Identity Management platformokkal együtt a COREid teljes körű megoldást nyújt az Oracle és az egyéb platformok és alkalmazások identitáskezelési feladataihoz.

ORACLE®

Oracle Hungary Kft.
Déli Point Irodaház
1123 Budapest,
Alkotás utca 17-19.

Telefon: +36 1 224 1700

Kereskedelmi információk: + 36 80 016 108

Fax: +36 1 214 0070

www.oracle.com/hu

Copyright © 2005, Oracle. Minden jog fenntartva.

Az Oracle, a JD Edwards és a Peoplesoft
az Oracle Corporation és/vagy társult
vállalatainak regisztrált védjegyei.