



PEOPLE COME FIRST
INFORMATIKAI SZAKÉRTŐK EGYESÜLETE

Oracle Identity Management

Az Identity Management rendszerek

- ▶ Az informatika világában az IDM (vagy IAM - Identity and Access Management) az a feladat, melynek kapcsán a szervezetekhez köthető felhasználókat (identitásokat), azok adatait és jogosultságait kezeljük
- ▶ Egy IDM rendszer lehetővé teszi a szervezeti menedzsereknek, hogy az egyes felhasználók információkhoz való hozzáférését hatékonyan irányíthassák
- ▶ Főbb feladatai egy ilyen rendszernek:
 - ▶ User lifecycle: A felhasználók „életciklusának” kezelése (létrehozás, menedzselés, törlés)
 - ▶ Authentication: Egységes belépési módszer biztosítása a szervezet alkalmazásaihoz, vagy akár egy több szervezetből álló domain alkalmazásaihoz is (Identity Federation)
 - ▶ Authorization: Jogosultságok nyilvántartása szerepkörökön (Roles) keresztül (ki? mit? mikor? miért?)

Miért előnyös az IDM egy nagyvállalatban?

- ▶ Automatizálja a manuális lépéseket a felhasználókezelésben
- ▶ Ezzel nagymértékben csökkenti az időt és költséget, amit a felhasználók kéréseinek teljesítésére kellene fordítani (jelszó módosítás, adatmódosítás, jogosultság kérés, stb.)
- ▶ A felhasználói élmény jelentősen javul a Self-Service portálok használatával
- ▶ Standard folyamatokat vezet be a szervezeti eljárások (házirend) betartására
- ▶ Az Auditálás (Auditing) és Riportolás (Reporting) egyszerűbbé válik

Oracle Identity Management

- ▶ Az Oracle Identity and Access Management egy termékcsalád, ami lehetővé teszi a szervezetek számára a felhasználók egységes és széleskörű kezelését a teljes életciklusuk alatt
- ▶ A felhasználóknak lehetőséget ad a szervezeti erőforrások irányított eléréséhez, ehhez Self-Service felületet biztosít
- ▶ Teljes körű eszköztárt ad az Authentication és Authorization szervezeti megvalósítására
- ▶ Biztosítja a több rendszerek, vagy akár több szervezetek közötti egységes adatáramlást és adatellenőrzést (Provisioning, Reconciliation, Certification)
- ▶ Az első termék az Oracle Internet Directory (1999) volt, ami egy LDAP implementáció. Ehhez az Oracle fokozatosan adta hozzá az évek során a komponenseket, kiterjesztve az IDM lehetőségeit
- ▶ Az aktuális verzió a 12c



Oracle IDM előnyei

- ▶ Az Oracle IDM közepes- és nagy-vállalatok számára ideális, ahol számítanak a növekedésre és komplex folyamatokkal rendelkeznek
- ▶ A termékcsalád egyes komponensei könnyen és támogatottan integrálhatók
- ▶ Igény esetén egyszerűen lehet új rendszereket bevonni az IDM folyamatokba
- ▶ Nagymértékben szabható a vállalati igényekhez
- ▶ A kezdeti fejlesztési költség magas lehet, ha a standard funkcionalitás nem elégséges a vállalat számára
- ▶ A dokumentáció széleskörű, de mélyre nyúló fejlesztések esetén konzultáns bevonására lehet szükség

Komponensek - OIM

- ▶ Az „Oracle Identity Manager” a felhasználókezelő rendszer központi alkalmazásainak összesége
- ▶ Magába foglalja a felhasználói Self-Service felületet (/identity), a rendszer adminisztrációs felületét (/sysadmin) és a folyamatok működését biztosító backend alkalmazásokat
- ▶ Az Identity Weblogic Domain része, dedikált Managed Server példányokon fut

Komponensek - SOA

- ▶ A Service-Oriented Architecture (Szolgáltatásorientált Architektúra) elve, hogy a hálózaton belül elérhető szolgáltatások egységes protokollon keresztül, egymástól függetlenül működve kommunikálhassanak egymással és az alkalmazásokkal
- ▶ Előre meghatározott kimenetelű üzleti folyamatokat definiálhatunk a BPEL (Business Process Execution Language) segítségével
- ▶ Az IDM-en belül a SOA komponens feladata a szervezet üzleti folyamatainak (Workflow) kezelése. Ilyen folyamat például a jogosultságok kérése, azok elfogadójának meghatározása
- ▶ Az Identity Weblogic Domain része, dedikált Managed Server példányokon fut

Komponensek - BIP

- ▶ Az Oracle Business Intelligence Publisher lehetővé teszi a szervezet felhasználói számára a riportok készítését, használatát és küldését
- ▶ Saját felhasználói felülettel rendelkezik (/xmlpserver)
- ▶ Az IDM Suite részeként a Standalone verzió áll rendelkezésre, extra licenc nélkül használható (ebből hiányzik sok extra funkcionális, például analitika, ami az OBIEE csomagban megtalálható)
- ▶ Az adatbázis vagy LDAP lekérdezések írásához adatmodell szerkesztő felületet biztosít, a riportok megjelenítéshez layout tervező áll rendelkezésre
- ▶ A riportokat generálhatjuk HTML, PDF, Excel, stb. formátumban
- ▶ A riportok generálását és küldését automatizálhatjuk az ütemező segítségével
- ▶ A jogosultságok kezelése egyszerűen kapcsolható az IDM-ben definiált szerepkörökhöz
- ▶ Az Identity Weblogic Domain része, dedikált Managed Server példányokon fut



Komponensek - OAM

- ▶ Az Oracle Access Manager feladata az erőforráselérés szabályozása
- ▶ Két fő területe:
 - ▶ Authentication - A felhasználók bejelentkezési kísérletének hitelesítése
 - ▶ Authorization - A hitelesített felhasználók erőforrásigényének vizsgálata
- ▶ A vállalat szintű bejelentkezések kezelését az Single Sign-On (SSO) technológiával támogatja
- ▶ Az Oracle HTTP Server-el a WebGate-en keresztül kommunikál
- ▶ Saját felületet biztosít az OAM szolgáltatások konfigurálásához (/oamconsole)
- ▶ Az Access Weblogic Domain része, dedikált Managed Server példányokon fut
- ▶ Igény esetén a domain egyéb szolgáltatásokkal egészíthető ki: Mobile Security, Adaptive Access Manager, Policy Manager



Komponensek - OHS

- ▶ Az Oracle HTTP Server egy Apache alapú webszerver
- ▶ Modulokkal egészítette ki az Oracle, amelyek kiterjesztik a funkcionalitását, például képessé teszik a Weblogic-cal való kommunikációra
- ▶ Képes terheléelosztásra (load-balance) több Weblogic példány között, vagy egy példány kiesésekor a kérések átirányítására (failover)
- ▶ IDM rendszerben „Reverse-proxy”-ként működik
- ▶ A WebGate plugin az OHS része, ezen keresztül kommunikál az Access Manager szerverekkel
- ▶ Ha van „SSL Termination”, akkor az lehet ezen a szinten, vagy a Load Balancer szintjén
- ▶ A Virtual Host-ok segítségével szeparáljuk az alkalmazásokat, például:
 - ▶ <https://idm.mycompany.com/identity>
 - ▶ <https://oimadmin.mycompany.com/sysadmin>



Komponensek - Adatbázis

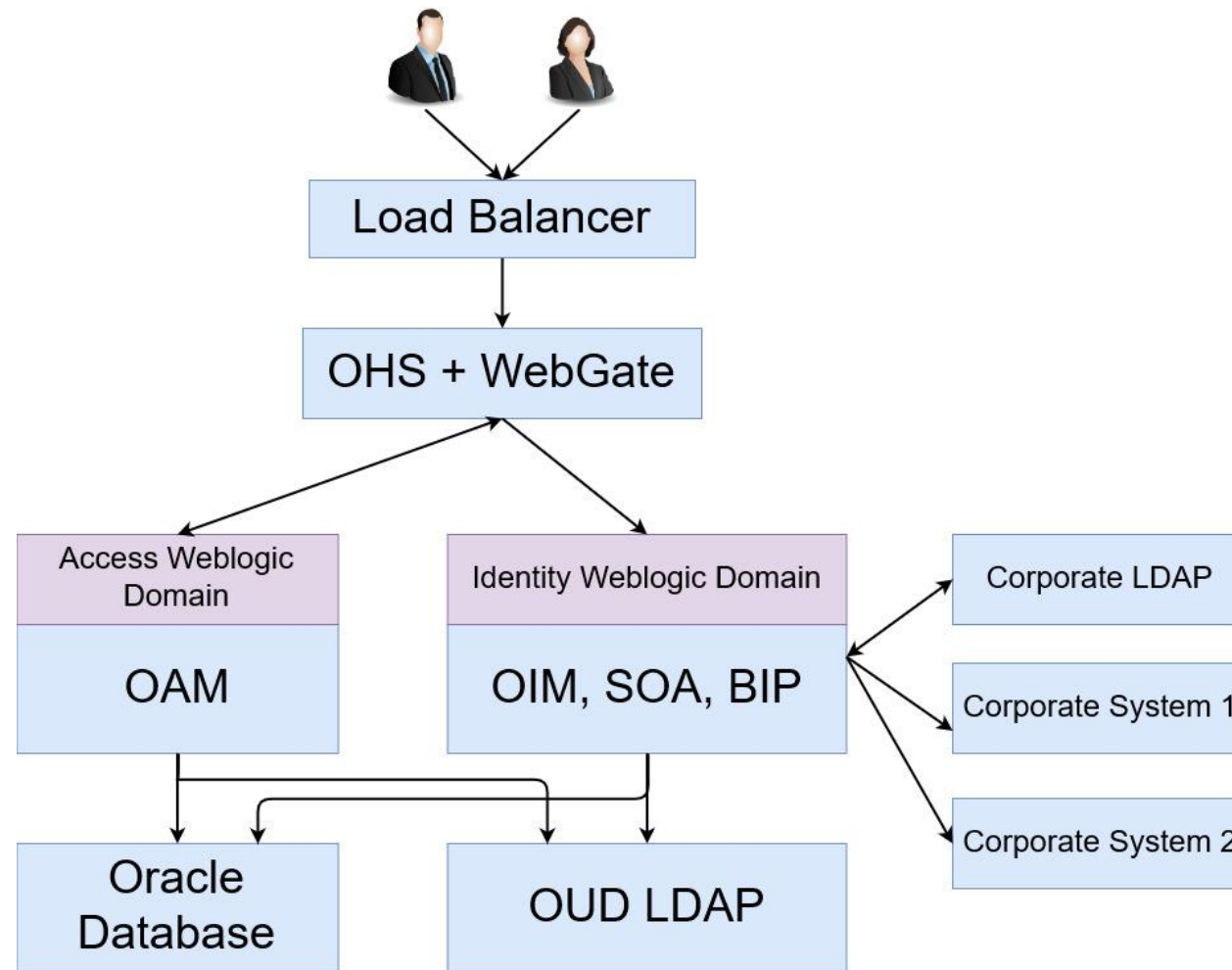
- ▶ Az IDM Suite telepítésének feltétele egy előre konfigurált Oracle adatbázis
- ▶ Minden komponens saját sémával rendelkezik
- ▶ A telepítő szoftver létrehozza a szükséges adatbázis felhasználókat, táblatereket és objektumokat
- ▶ Minden, a felhasználókhoz és a rendszer működéséhez köthető adat (OIM Metadata) itt van eltárolva

Komponensek - OUD

- ▶ Oracle Unified Directory - újgenerációs LDAP (Lightweight Directory Access Protocol) kezelő szoftver, amit az Oracle a Sun OpenDS-ből alakított ki
- ▶ Az adatokat fájlokban tartja (szemben az Oracle Internet Directory-val, ami egy Oracle adatbázisban tárolja az adatokat)
- ▶ Képes proxy-ként működni a kliens és egy másik LDAP szerver között
- ▶ Szinkronizálhatja (replikálhatja) az adatokat más LDAP szerverek felé (vagy több OUD példány egymás között)
- ▶ Az IDM rendszerben az OUD tárolja a felhasználók legfontosabb adatait és jogosultságait. Identity Store-nak is hívjuk
- ▶ Bejelentkezéskor a felhasználót az OUD-ban tárolt adatok alapján hitelesíti az Access Manager
- ▶ Ez a kapcsolati pont az OIM és az OAM között



IDM architektúra

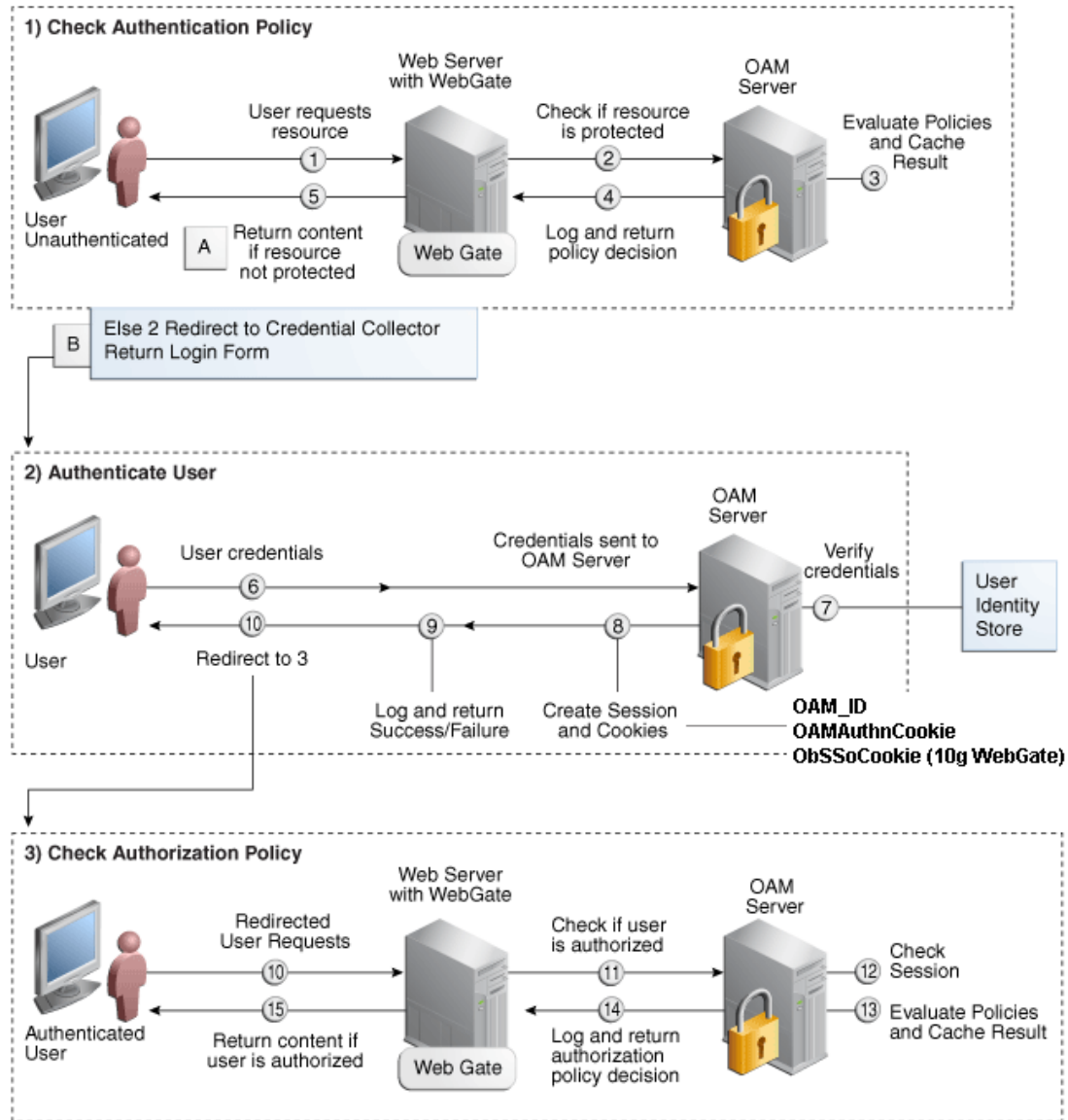


Az OIM Telepítése

- ▶ Több lehetőség van:
 1. Kézzel telepítjük és konfiguráljuk az egyes komponenseket. A dokumentáció részletes, de időigényes munka, tele hibalehetőséggel
 2. 12c-től kezdve: Quick Installer
- ▶ Frissítések: az OPatch szoftverrel telepíthetjük a javításokat, minden komponenshez külön-külön
- ▶ Javítócsomagok (Bundle Patches) három havonta érkeznek
- ▶ Egy-egy hiba javítását one-off patch-nek hívjuk

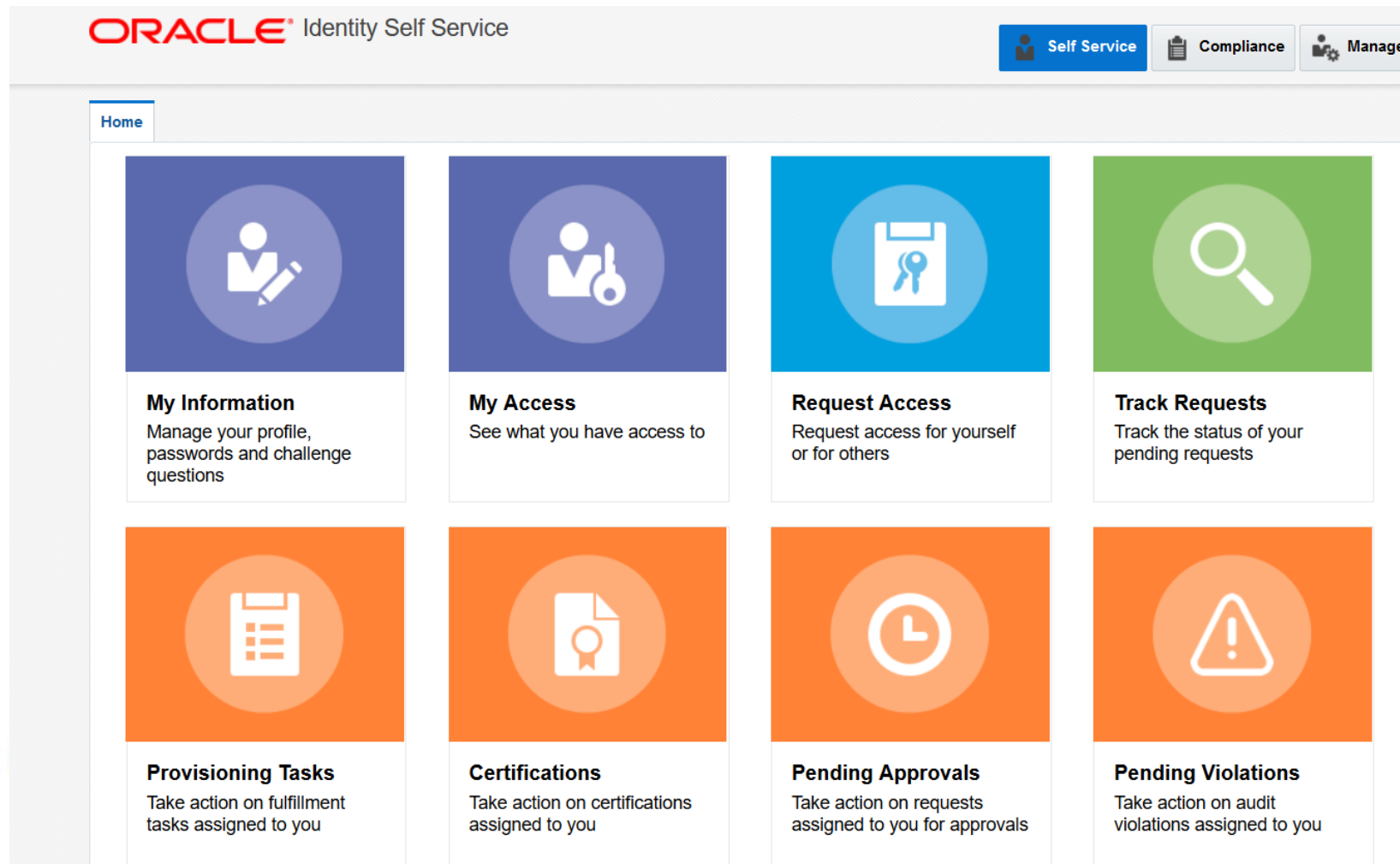


A bejelentkezés folyamata



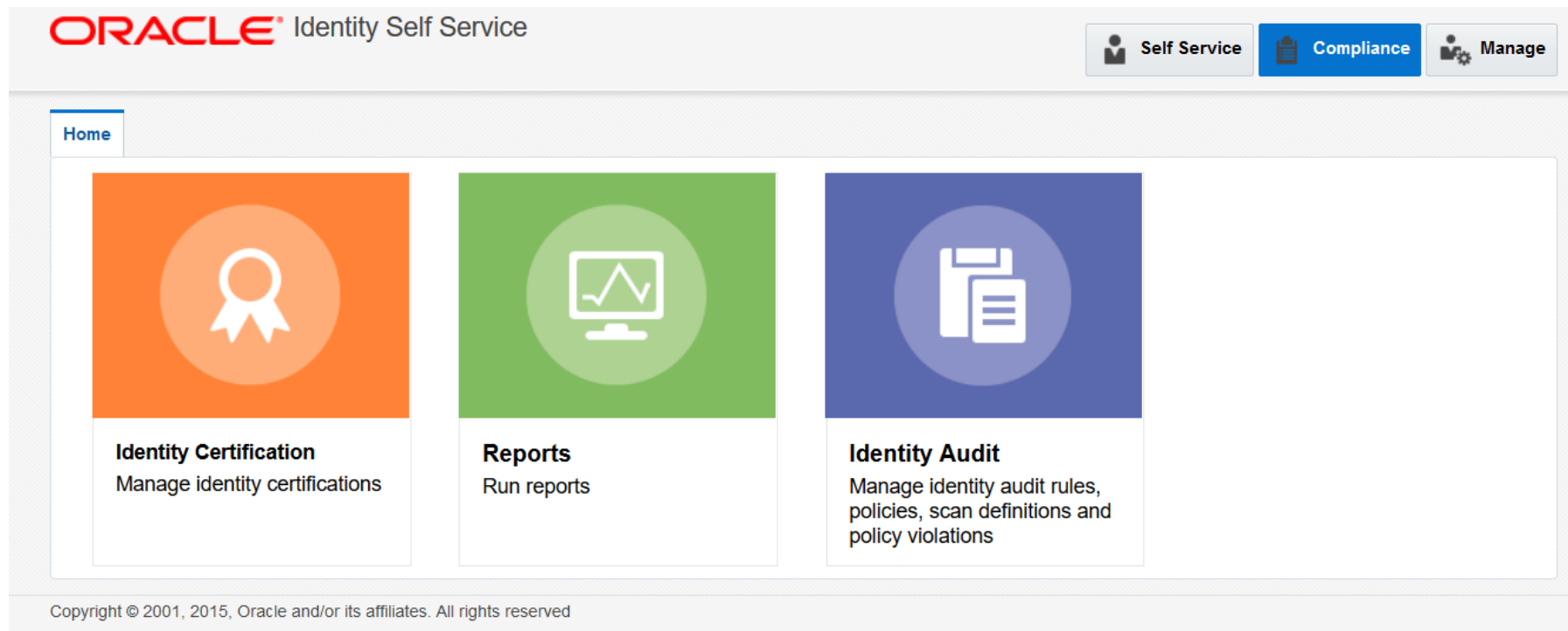
Az OIM felülete I

- ▶ Az OIM Identity front-end alkalmazásban, a „Self Service” oldalon a felhasználó a hozzá kötődő adatokat tekintheti meg, illetve kezelheti őket



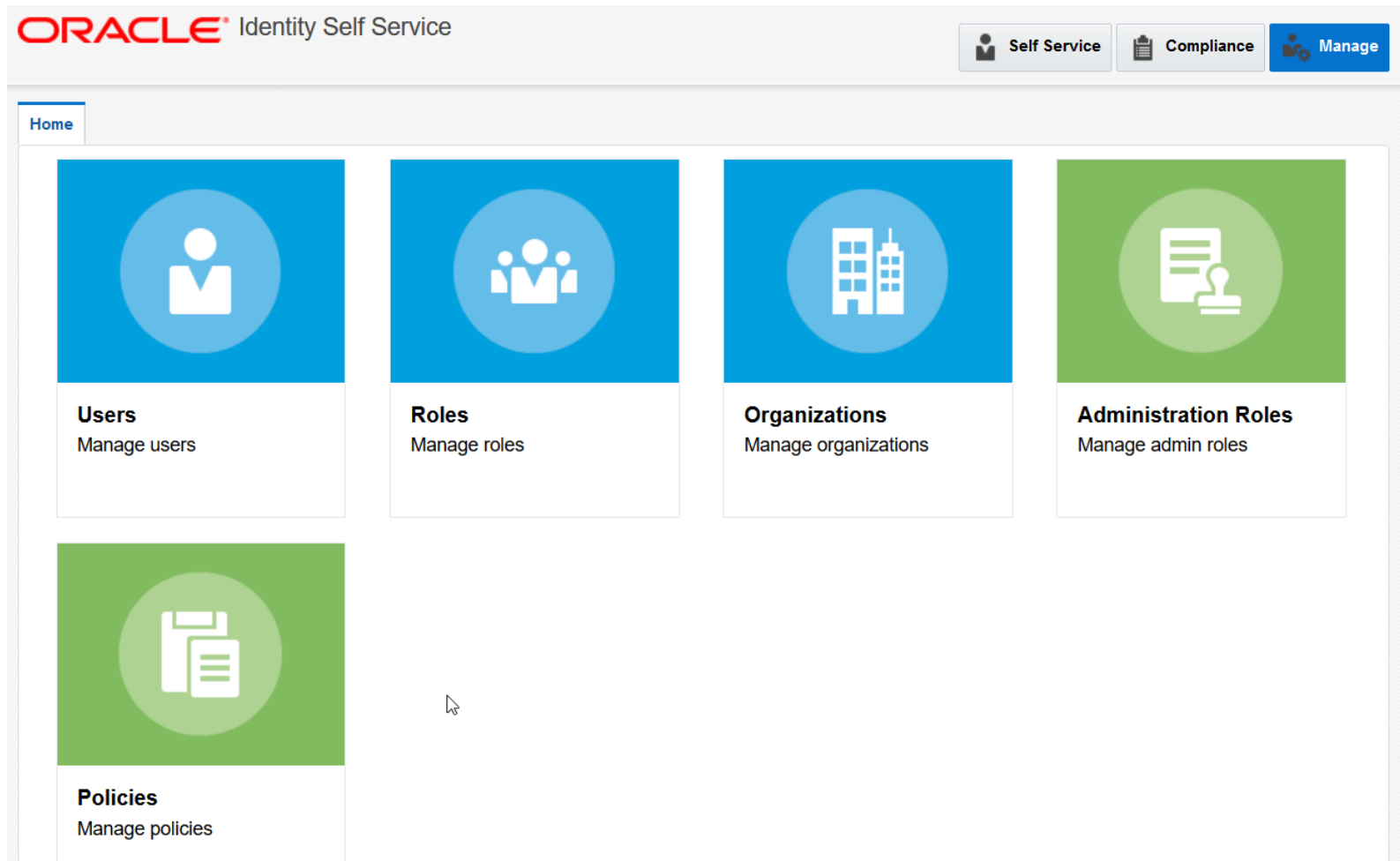
Az OIM felülete II

- ▶ A „Compliance” oldal az üzleti adminisztrátorok számára biztosítja a minősítések (Certification) ellenőrzését

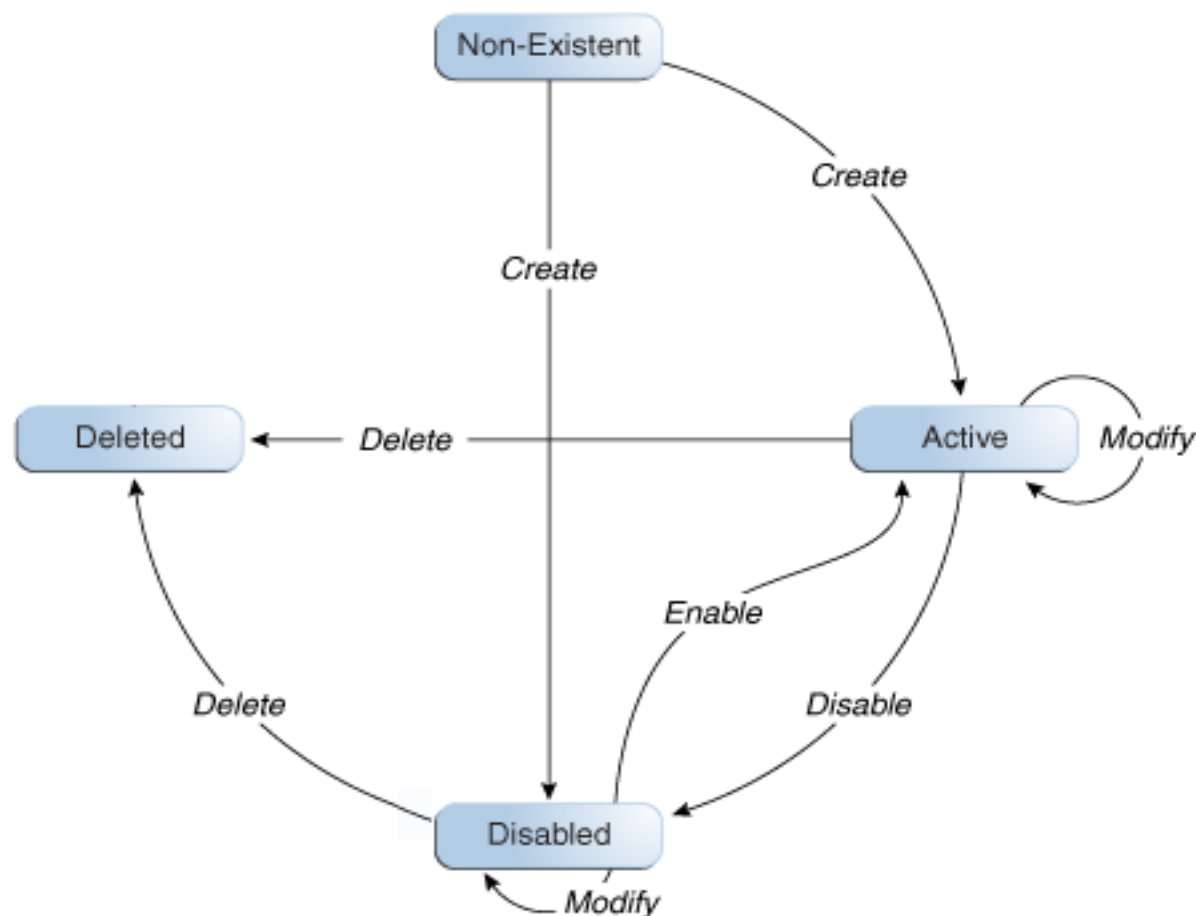


Az OIM felülete III

- ▶ A „Manage” oldal az üzleti adminisztrátorok számára biztosítja a felhasználók, jogosultságok és szervezeti „házi rend” kezelését



A felhasználók életciklusa



- ▶ Minden felhasználónak egyedi azonosítója van (UserID)
- ▶ A felhasználók lehetnek még zárolt vagy nem zárolt állapotban is (Locked/Unlocked)
- ▶ Még törölve sem tűnnek el a rendszerből
- ▶ Minden felhasználó egy szervezet (Organization) alá van besorolva

Jogosultságok

- ▶ Három féle jogosultságot különböztetünk meg az OIM-ben, a vállalat dönti el, hogy ezek közül melyiket használja
 - ▶ **Roles:** Szerepkörök, amelyek hierarchiába is rendezhetők. Ha van bekötve Identity Store (OUD), akkor ott is létrejönnek, mint egy LDAP csoport, a rendszer pedig a felhasználókat a csoportokhoz rendeli. Az LDAP-on keresztül ezeket a szerepköröket más Oracle komponensek is ellenőrizhetik.
 - ▶ **Entitlements:** jogosultságok, amelyek szinkronizálásra kerülnek más kapcsolódó rendszerekhez.
 - ▶ **Admin Roles:** Az Admin szerepkörökön keresztül adhatunk bizonyos felhasználóknak képességet (capability) az OIM funkcióinak elérésére. Ilyen lehet például a felhasználók létrehozása, törlése. Az OIM elrejtí a funkciógombokat, amiket a felhasználó nem érhet el
- ▶ Felhasználói fiókok (Accounts): a kapcsolati pont a felhasználó más rendszerekben létező identitásai között. Rendszerenként lehet egy vagy több fiók is felhasználónként



Jogosultság igények

- ▶ Minden felhasználó kérhet saját magának jogosultságokat, vagy akár mások számára is
- ▶ Az igényelni kívánt jogokat a katalógusból (Catalog) lehet kiválogatni
- ▶ A webáruházak „bevásárlókosár” elvén működik
- ▶ Ha az igény (Request) átesik az OIM oldali ellenőrzésen, és elküldésre kerül, akkor a SOA elindít egy folyamatot (Workflow) és ennek kapcsán meghatározza azt a felhasználócsoporthat, akik a kérést elfogadhatják
- ▶ Ez több szinten is történhet (például „négy szem elv” esetén)

Adatok szinkronizálása más rendszerekkel

- ▶ **Provisioning:** Az OIM által módosított felhasználói és szervezeti adatok küldése a kapcsolódó rendszereknek
- ▶ Tipikusan az OIM kezdeményezi a küldést (Push modell) egy módosítás hatására
- ▶ **Trusted Reconciliation:** Új felhasználók betöltése (létrehozása) az OIM-ben a kapcsolódó rendszerek adatai alapján
- ▶ **Target Reconciliation:** A felhasználók kapcsolódó rendszerekhez tartozó fiókjainak adatait tölti be a kapcsolódó rendszerben történt változások alapján
- ▶ A reconciliation lehet push vagy pull modell alapú. Pull modell esetén az OIM ütemezetten kéri le az adatokat



Identity Connector Framework

- ▶ Az ICF egy egységes, köztes réteget képez az OIM és a célrendszerek között az adatcsere végrehajtásához (provisioning, reconciliation)
- ▶ A létrehozott Connector implementációk függetlenek az alkalmazástól, izoláltan tesztelhetők
- ▶ A keretrendszer két rétegből áll:
 - ▶ API (Application Programming Interface): Ezt a réteget hívják az alkalmazások. Független a tényleges Connector működéstől, elfedi azt
 - ▶ SPI (Service Provider Interface): A fejlesztők az SPI réteg azon interfészeit implementálják, amelyek szükségesek a célrendszer támogatásához
- ▶ Az Oracle sokféle Connector-t biztosít (Active Directory, SAP, Flat File, Office 365 stb.)
- ▶ Ha egy rendszerhez nincs Connector, akkor a keretrendszer segítségével fejleszteni kell egyet



Identity Certification

- ▶ A Certification az a folyamat, amelynek kapcsán ellenőrzik a felhasználóknak kiosztott jogosultságok és hozzáférhetőségek helyességét
- ▶ A folyamat kimenetele lehet a jóváhagyás, vagy elutasítás, ami a kérdéses jogok elvételével jár
- ▶ Az OIM rendszerben indítható egyes felhasználókra (User Certification), vagy egyes jogosultságok birtoklóira (Entitlement- vagy Role-Certification).
- ▶ Minősítési feladatok létrejöhetnek ütemezetten, vagy Event Trigger hatására (például kiválthatja felhasználók módosítása)
- ▶ A minősítést végző felhasználók számára külön felületet biztosít

Az OIM Ütemező

- ▶ Az OIM Scheduler felel az előre meghatározott feladatok (Jobs) ütemezett teljesítéséért
- ▶ Ezek típusai:
 - ▶ OIM specifikus feladatok, amelyek a rendszer karbantartásáért vagy funkcionalitásáért felelnek (például régi audit bejegyzések törlése vagy lejárt jelszavak ellenőrzése)
 - ▶ LDAP Reconciliation feladatok, amelyek az OUD-ban észlelt módosításokat betöltik az OIM rendszerbe (ilyen módosítás lehet például, amikor az Access Manager zárol egy felhasználót az elűtött jelszavak miatt).
 - ▶ Saját fejlesztésű ütemezett feladatok, például a kapcsolódó rendszerek adatainak betöltéséhez

Auditing

- ▶ Minden vállalat számára kritikus az IT rendszeren belül történt események rögzítése, naplózása
- ▶ Az OIM beépítetten képes felhasználók, jogosultságok és a katalógus auditálásra. Ezek szintjei (az audit részletessége) is állítható
- ▶ Ezen kívül az Oracle Fusion Middleware legtöbb komponenséhez beállítható auditálás:
 - ▶ Ezt a Weblogic kezeli és az Enterprise Manager-ben konfigurálható
 - ▶ Külön adatbázis sémát kell létrehozni az OIM és OAM audit számára, ide töltődnek be az adatok
 - ▶ Az Access Manager Auditing beállítása esetén például bejegyzések készülnek minden URL elérésekor, bejelentkezéskor vagy kilépéskor, felhasználónévvel és IP címmel ellátva



Monitoring

- ▶ Mind a rendszer komponenseinek működését, mind az alkalmazás funkciókat érdemes felügyelni
- ▶ Ellenőrizni kell az operációs rendszer erőforrásait
- ▶ A futó Weblogic példányok figyelésében segít az Enterprise Manager vagy írhatunk WLST szkripteket is
- ▶ Visszatérő hibák kiszűrésére érdemes lehet beütemezni szkripteket, amik az alkalmazás logokat olvassák
- ▶ Az OIM funckiók (hibás provisioning feladatok, beragadt jogosultság igények) felügyeletére érdemes BIP riportokat generálni, amik az adatbázis táblákból kérdeznak le (de az adminisztrátorok az OIM felületén is át tudják ezeket nézni)

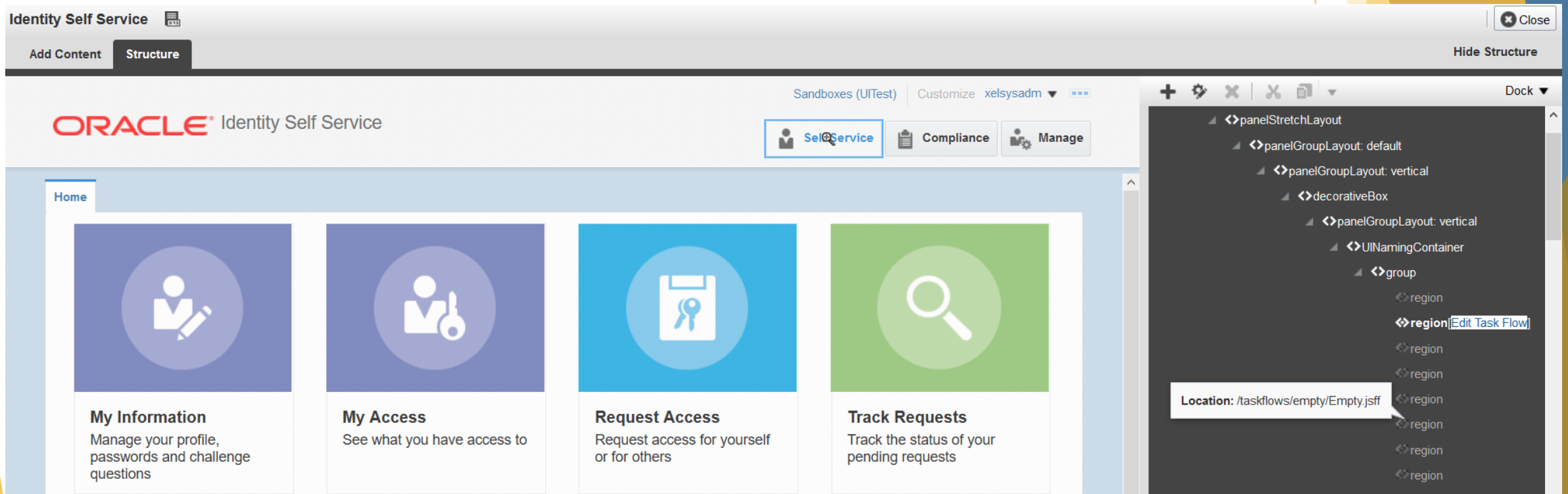
A rendszer konfigurálása

- ▶ Telepítés után alapesetben a xelsysadmin felhasználó használható az OIM teljeskörű adminisztrációjához
- ▶ A „System Administrator” Admin Role neki van kiosztva
- ▶ Beléphetünk vele a /sysadmin felületre, innen érhetjük el az ütemezőt, a rendszerbeállításokat, telepíthetünk Connector-okat, módosíthatjuk a meta-adatokat (export-import) stb.
- ▶ Több száz attribútumot állíthatunk, amelyek befolyásolják a rendszer működését
- ▶ Az Enterprise Manager segítségével még részletesebb szoftverbeállításokat alkalmazhatunk
- ▶ Minden beállítás az adatbázisban van eltárolva



Fejlesztés I - UI

- ▶ A felhasználó felület könnyen változtatható a böngészőben is
- ▶ A módosítások a Sandbox funkcionalitás segítségével menthetők el
- ▶ Saját kód hívásához: ADF alapú Java Managed Bean-ek létrehozása és ezek hívása az Expression Language segítségével. A fejlesztés JDeveloper környezetben történik



Fejlesztés II - Sandbox

- ▶ Ahhoz, hogy a megjelenítési felülethez kötődő változtatásokat eszközöljünk, készítenünk kell egy Sandbox példányt
- ▶ Egyszerre mindig csak egy példány lehet aktív, ez rögzíti az elvégzett változtatásokat (módosításokat a metaadatokban)
- ▶ A Sandbox lényegében egy zip fájl könyvtárakkal és xml fájlokkal
- ▶ Az elkészített Sandbox exportálható (és importálható egy másik rendszerbe) vagy publikálható. Publikálás esetén minden módosítás rögzül a rendszerben
- ▶ Érdemes teljes metadata mentést készíteni publikálás előtt
- ▶ Több Sandbox példány között gyakran van függőség: figyelni kell a sorrendre, ha például teszt rendszerből éles rendszerbe importáljuk őket. Könnyen felülírhatunk változásokat, ha nem a megfelelő sorrendben kerülnek ki a SandBox-ok

Fejlesztés III - Backend

- ▶ Az OIM backend fejlesztése különféle feladatokból áll
 - ▶ SOA Workflow fejlesztés: a JDeveloper biztosítja a környezet a BPEL alapú logika előállításához
 - ▶ Connector implementációk létrehozása
 - ▶ Provisioning vagy Reconciliation feladatok elvégzéséért felelős objektumok létrehozása
 - ▶ Ezeken felül az OIM szinte minden működési területét át lehet alakítani vagy bővíteni lehet saját kód bekötésével

Fejlesztés IV - Rest API

- ▶ Gyakori igény, hogy a távoli alkalmazások is képesek legyenek műveleteket végrehajtani az OIM rendszerben. Két lehetőség:
 - ▶ OIM Java API hívások: A távoli alkalmazás t3 protokollon keresztül, kliensként hívja az OIM interfészeket
 - ▶ OIM REST (Representation State Transfer) API hívások: SCIM (System for Cross-Domain Identity Management) protokoll alapú Webservice hívások HTTP-n keresztül
- ▶ Ha a kérések csak Load Balancer-en keresztül érkezhetnek, a direkt API hívások csak körülményesen oldhatók meg
- ▶ Az OIM REST szolgáltatásokon keresztül az OIM funkciók nagy részét elérjük: felhasználók, jogosultságok, szervezetek kezelése vagy akár a rendszer módosítása

OIM Tuning

- ▶ Az optimalizálás főbb feladatai:
 - ▶ Adatbázis hangolása a megfelelő paraméterek beállításával
 - ▶ Az OIM szoftver beállításainak finomhangolása (pl.: object caching)
 - ▶ Weblogic Tuning: a JVM indító paramétereinek módosítása, Work Managerek és adatbázis kapcsolatok (Datasources) hangolása
- ▶ Iránymutatóként az Oracle készített tuning dokumentációkat



Köszönöm a figyelmet!

- ▶ Elérhetőségem: peter.joo@webvalto.hu

