

Networkshop 2011

Jogosultság-monitorozó rendszer kialakítása

Jogosultságkezelés jelentősége

- Miért fontos?
 - ▣ Mindenkinek van valamilyen válasza
 - ▣ A válaszok különböző megközelítésűek lehetnek
 - ▣ Egy közös pont: **Kockázatok csökkentése**



Jogosultságkezelés jelentősége

- Eszköz az adatvagyon védelmére
- Biztonságtudatosság
 - ▣ Kockázatok felmérése, tudatosítása, csökkentése
- Jogosultságok kézben tartása mint kockázatcsökkentés
 - ▣ Belső kényszer
 - ▣ Külső szabályozások (PSZÁF, ISO)

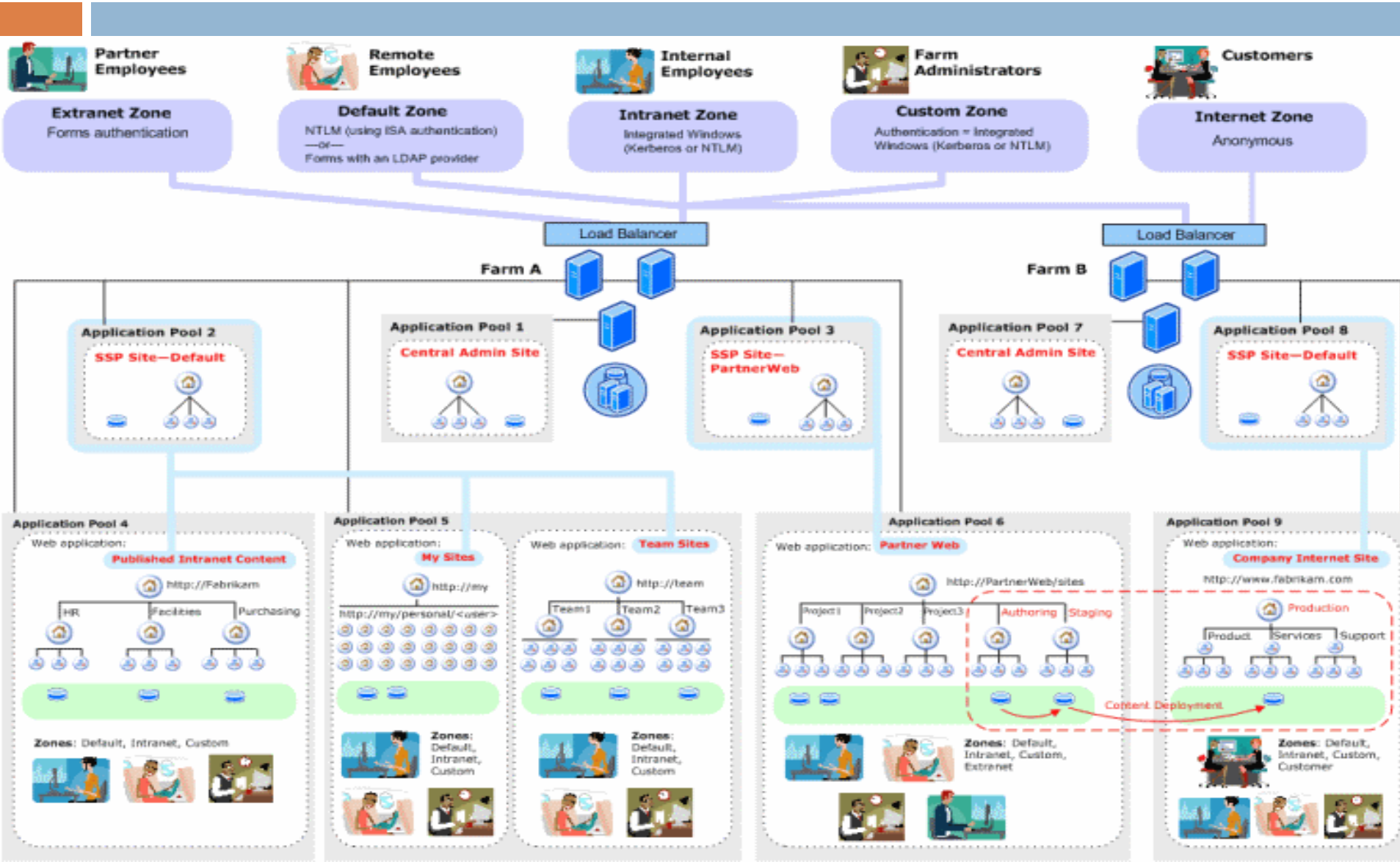


Jogosultságkezelési kockázatok

- Alacsony minőségű jogosultságkezelés
- Plusz jogok
 - ▣ **Indokolatlan jogok kiosztása**
 - ▣ Jogok visszavonásának elmaradása
- Erős jogkörrel rendelkező felhasználók önhatalmú működése



Példa jogosultsági struktúrára



Gyakori kérdések

- Melyek azok a felhasználók, akik több jogosultsággal rendelkeznek, mint amit munkakörük megkíván?
- Egy adott felhasználó milyen fájlokhoz és rendszerekhez férhet hozzá és milyen jogosultsági szinttel?
- Milyen felhasználók rendelkeznek teljes adminisztrációs jogkörrel?
- Milyen technikai felhasználók léteznek és milyen jogkörrel rendelkeznek?
- Milyen inaktív account-ok találhatóak a rendszerekben?

A fő probléma

- Manuális módszerrel áttekinthetetlen beállítások
 - ▣ Öröklődő jogosultságok miatti káosz
 - ▣ Ad-hoc beállítások
 - ▣ Csoportjogtól eltérő jogok



**Nincs információ
a tényleges helyzetről**

Ismert megoldások

- Egyedi, manuális jogosultságkezelés
- Központi jogosultságkezelés
 - ▣ Belső szabályozással (nem hatékony)
 - ▣ Teljeskörűen, elektronikusan (drága)
- **Tényleges jogok felolvasása – nem igazán elterjedt megoldás**

Megoldási javaslat

Induljunk ki a tényleges helyzetből!

- A kialakítandó rendszernek képesnek kell lennie
 - ▣ A pillanatnyi jogosultságok föltérképezésére
 - ▣ A beállított jogosultságok védett adatbázisban történő tárolására
 - ▣ Standard és adhoc jellegű riportok készítésére a belső összefüggések feltárására

A rendszerrel szemben támasztott elvárások

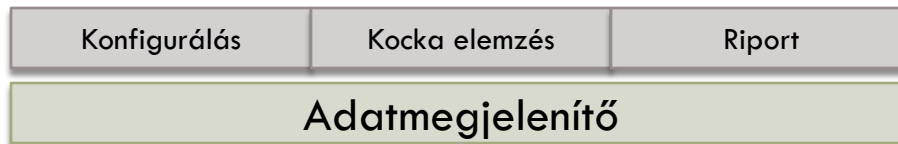
- Legyen moduláris és skálázható
- Mutassa meg az eltérést a tényleges helyzet és a vezetői szándék között
- Biztosítsa az adatok monitorozását és összetett elemzését
- Rendelkezzen fejlett riportolási képességekkel

Elméleti felépítés

- A kialakítandó rendszer tulajdonképpen egy adattárház lesz, mivel:
 - ▣ Különböző adatokat, különböző helyről gyűjtünk össze egy adatbázisba (ETL)
 - ▣ Az adatokon transzformációkat végzünk és közös alapokra hozzuk őket (OLAP)
 - ▣ Az adatok több dimenzión keresztül is elérhetőek, megjeleníthetőek (Kocka)
 - ▣ A több dimenziós adatok egy-egy nézetéről pillanatfelvétel készíthető (Riport)

Valós felépítés

Adatmegjelenítő - elemző (Security Manager – Kocka, Riport)



Adattároló (Store Server - OLAP)



Felfedezők (Discoverer - ETL)



Adat források

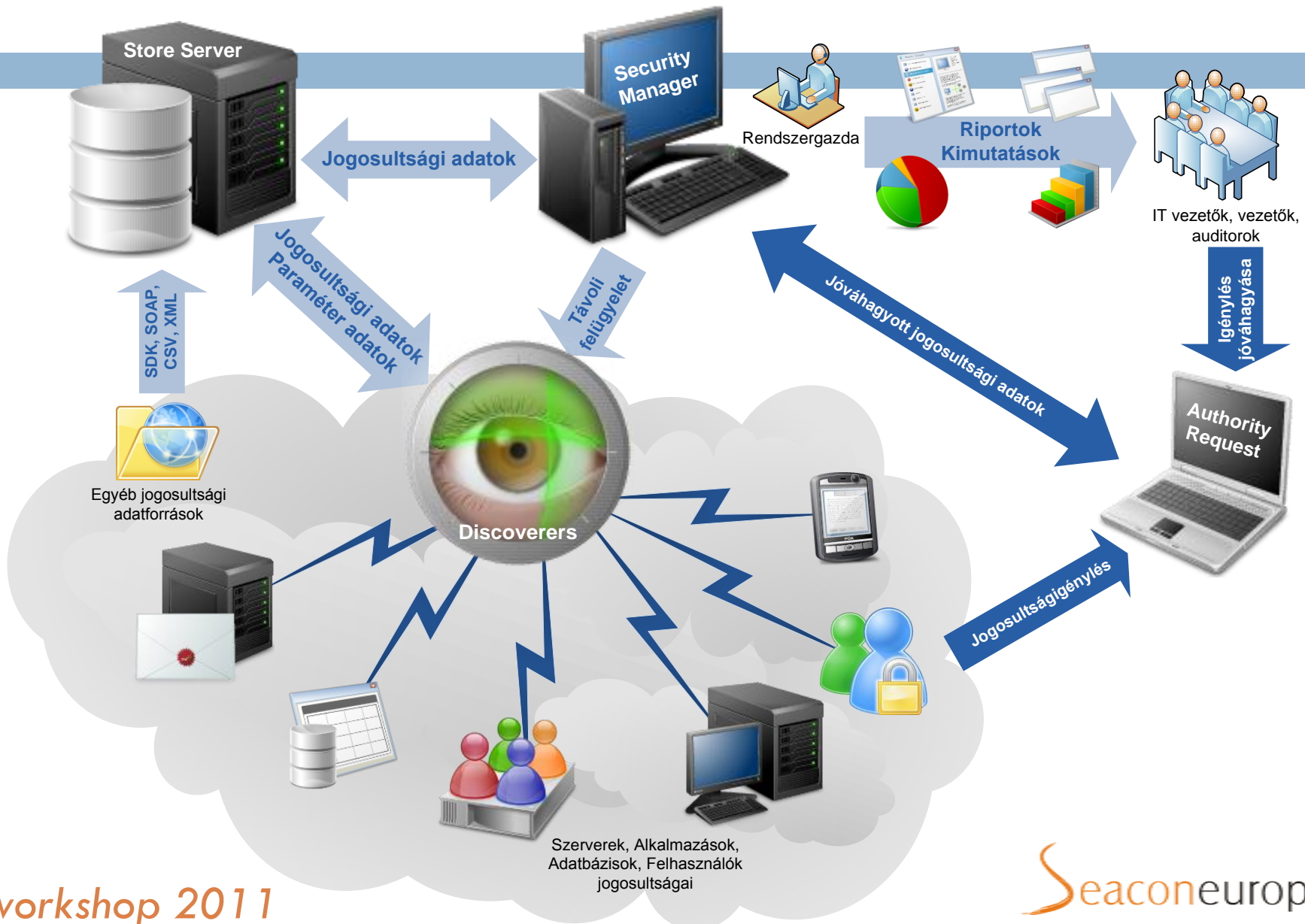


C:\Dokumentumok
\\Seacon\Seacon

Srvportal\Sarm
Srvportal\Helpdesk

http://intranet
http://project

Működési ábra



Felhasználási példák

- Rendszerüzemeltetők, rendszergazdák
 - Elemzések készítése
 - Anomáliák felderítése
 - Elvégzendő feladatok listája
- IT vezetők, vezetők
 - Előre definiált jelentések, statisztikák
- Auditorok
 - Megfelelőségi riportok

Bevezetési alapelvek

- Informatikai stratégia és IT biztonsági szabályozással összhangban
- Kockázatfelmérés alapján kritikus rendszerek mentén
- Vállalat működési folyamataiba integrált módon



Köszönöm

a

figyelmet!

csizmadia.attila@seacon.hu
www.sarm.hu