Security Intelligence.
Think Integrated.

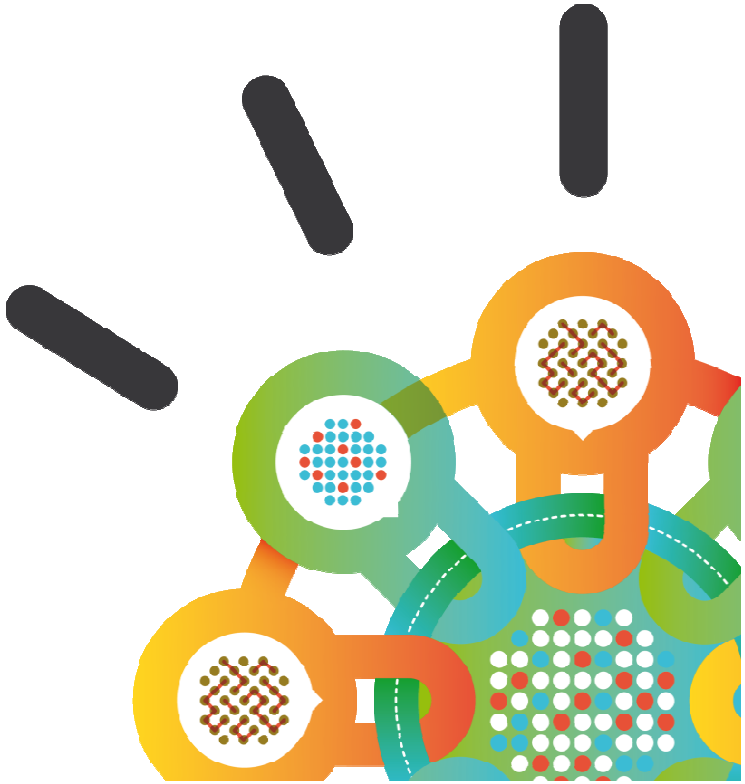
IBM Security Privileged Identity Manager

Biztonságos gyökérkezelés

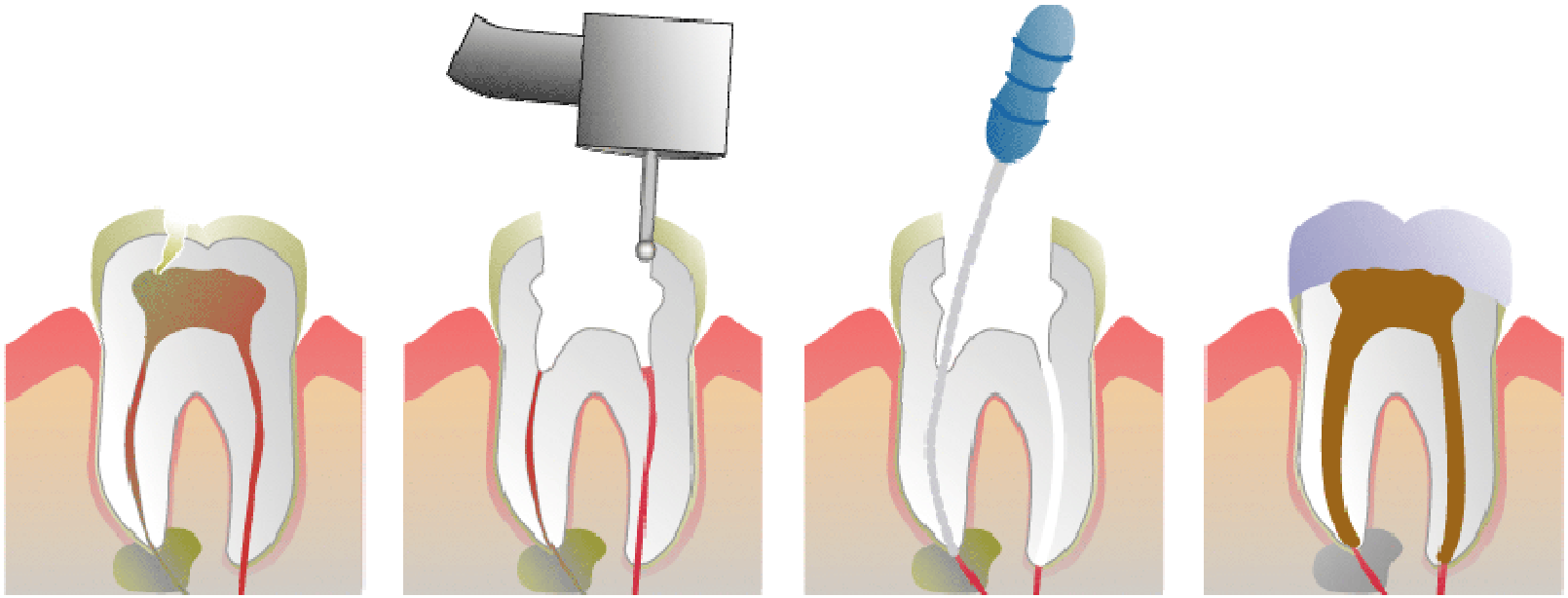
HuTUG – 2013 szeptember 20.

Nagy Gergő

IBM biztonsági szoftver specialista



Gyökérkezelés

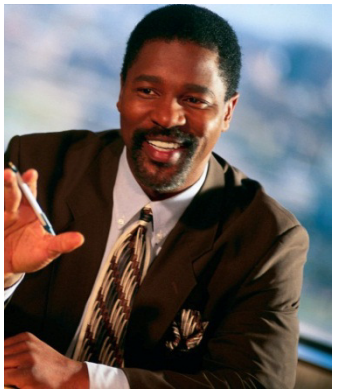


- *„A gyökérkezelés során a fogbélüreg (pulpa) tartalmát eltávolítják ezt a teret lehetőség szerint sterillé teszik, és olyan anyaggal tömik be a gyökércsatorna teljes hosszában, amely tartós zárást biztosít.”* Wikipedia

© 2013 IBM Corporation

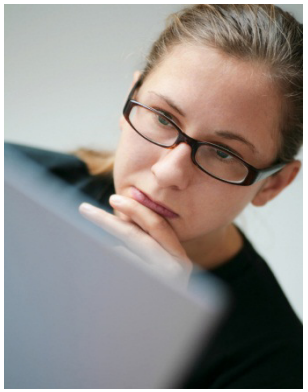
Kik azok a privilégizált felhasználók?

- Érzékeny erőforrásokhoz speciális előjogokkal hozzáférő felhasználók
- Kockázatot jelentenek:
  - Gondatlanság
  - Szándékos károkozás
- Példák: (nem csak System Admin)
  - Root
  - Oracle Financials Admin
  - Directory Server Admin
  - Unix File Shares Admin
  - DB2, SQL Server Admin
  - AD Domain Admin
  - SAP Admin
  - Security Infrastructure Admin
  - Firewall account access



Alkalmazásgazdák

IT Adminisztrátorok



DB Adminisztrátorok

© 2013 IBM Corporation

A privilégizált felhasználó-kezelés problémái (hagyományos megközelítés)

Minden adminisztrátornak saját fiók minden rendszerben

- Exponenciálisan növekvő privilégizált fiókok
- Privilégizált fiókok helytelen kezelésének kockázata
- Növekvő fiókszám adminisztrációs költsége

Adminisztrátorok megosztott privilégizált fiókkal

- A felelősségre vonhatóság lehetősége elveszik
- Jelszókezelési és biztonsági problémák
- Szabályozási elvekkel ellentétes megközelítés

Megoldás szükséges a privilégizált felhasználók elszámoltathatóságára, a fiókok szabályozására és automatizációjára

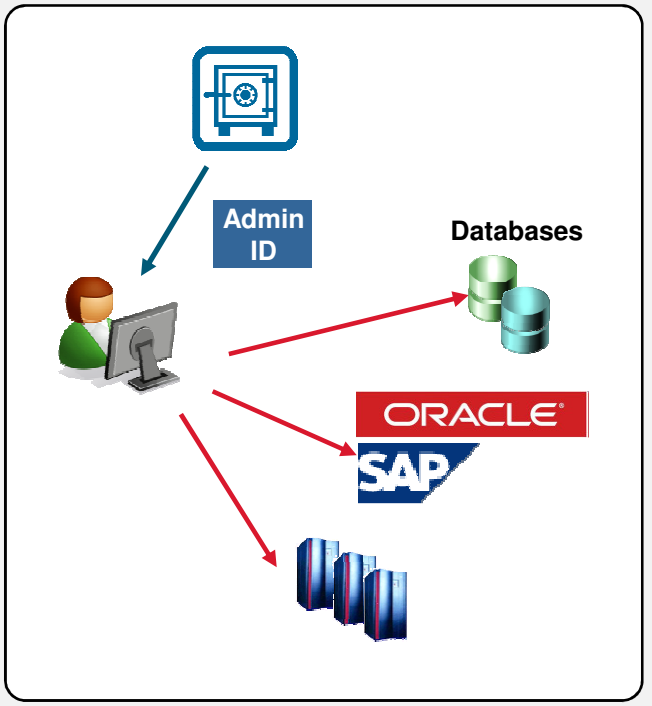
© 2013 IBM Corporation

IBM Security Privileged Identity Manager

A megosztott identitások központi kezelése, auditálása

- ***Szabályozott hozzáférés a megosztott érzékeny fiókokhoz***
  - *„Check-in / check-out” biztonságos credential vault használatával*
- ***Hozzáférés igénylés, jóváhagyás and újraérvényesítés***
  - *Kockázat csökkentés, megfelelőség*
- ***A megosztott ID-k nyomonkövetése***
  - *Elszámoltathatóság*
- ***Automatizált jelszókezelés***
  - *Automatizált ID checkout, a jelszó elrejtése az igénylőtől, automatizált jelszó reset*

IBM Security Privileged Identity Manager

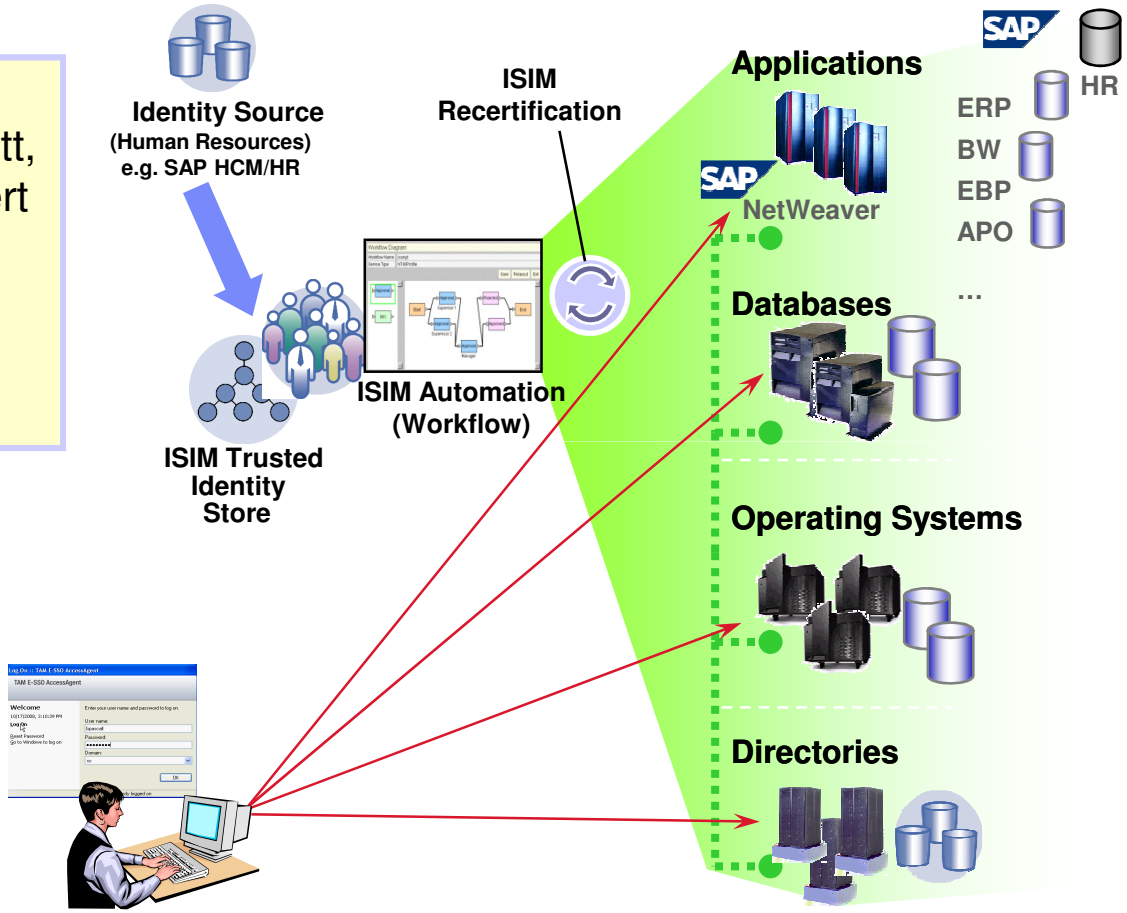


© 2013 IBM Corporation

Működése

- Az IBM Security Identity Manager felelős a megosztott, privilégizált fiókok kezeléséért
  - Fiók életciklus
  - Pool-ba rendezés
  - Jóváhagyatás

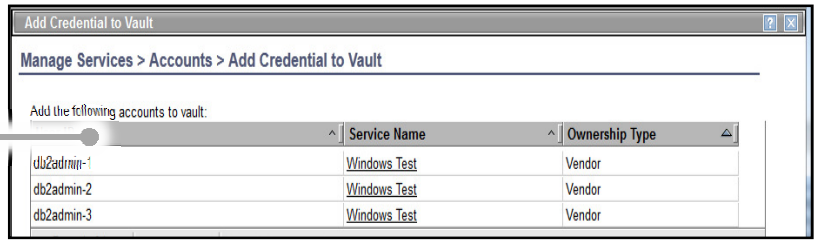
- Az SSO Agent komponens felelős a következőkért:
  - Automatizált beléptetés
  - Check-out/in
  - Naplózás



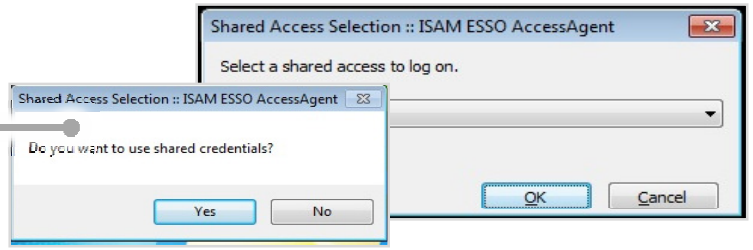
© 2013 IBM Corporation

Működése (folyt.)

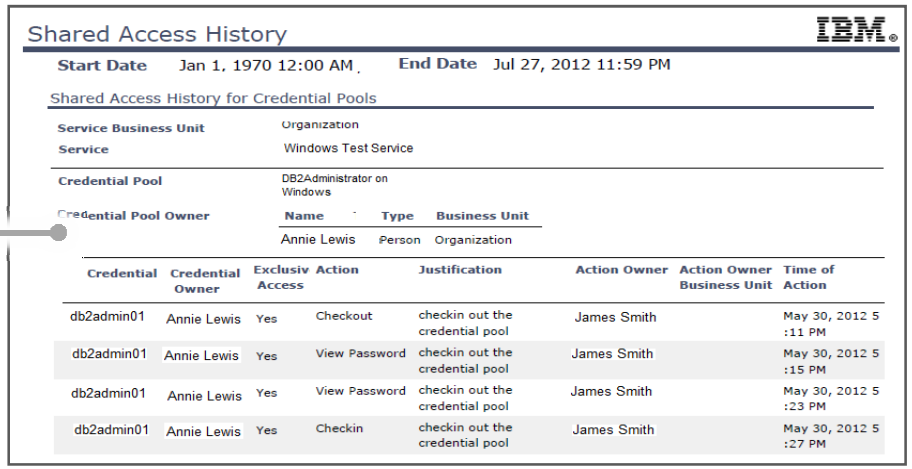
1. Privilégizált fiók konfiguráció



2. A generált jelszó automatikusan elérhetővé válik/„check-out”-ol. Kijentkezéskor a jelszó automatikusan visszakerül/check-in”-el a credential vault-ba.



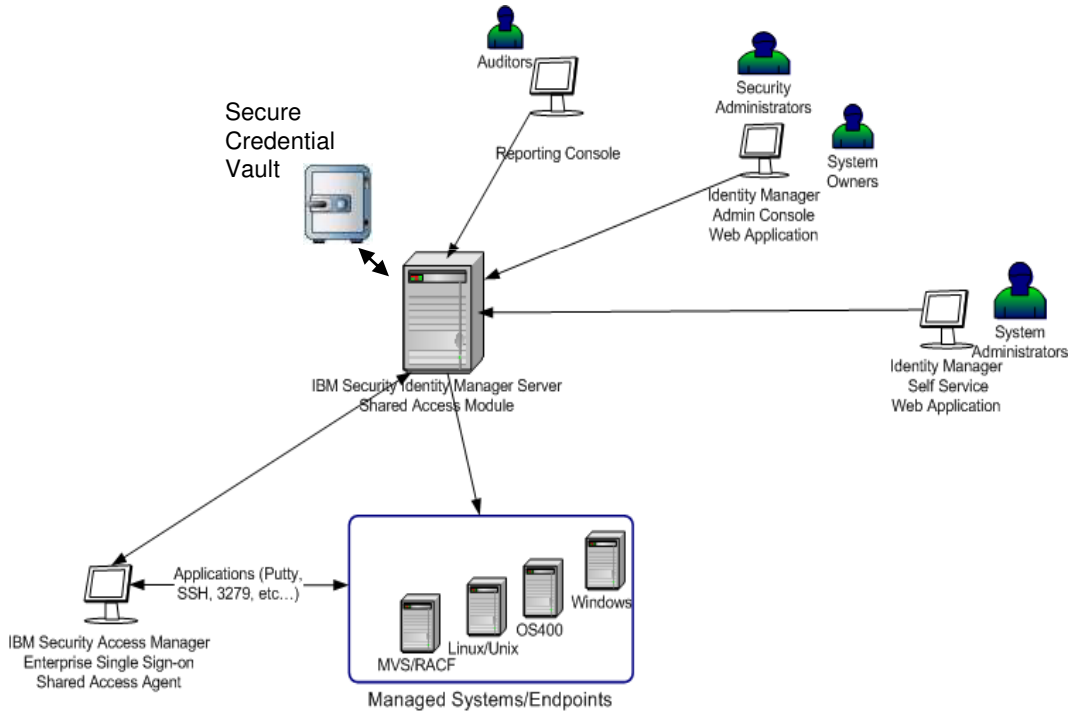
3. Felhasználói tevékenységek naplózása



A technológia az IBM Security Identity Manager és Enterprise Single Sign-On együttes képességein és integrációján alapul

© 2013 IBM Corporation

Szoftver komponensek



IBM Security Identity Manager - Shared Access Module

- Új Identity Manager 6.0 komponens, ami felelős a PIM kiterjesztésért
- Telepítés az IBM Security Identity Manager telepítéssel egyidőben vagy utólag.

IBM Security Access Manager for Enterprise Single Sign-on - Privileged Identity Manager Agent

- Új komponens az IBM Security Access Manager Enterprise Single Sign-on 8.2-ben.
- Beépített kliens modullal kommunikál az ISIM PIM Web Service-szel.
- Automatizált check-out és check-in képesség.

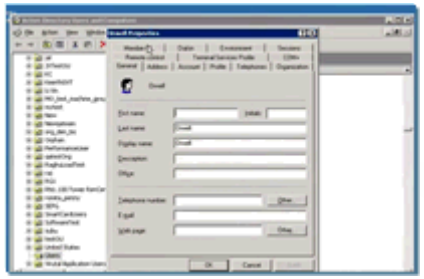
© 2013 IBM Corporation

Privileged Session Recorder

1 **Checkout PIM credential, bejelentkezés a végpontba** (privileged user)

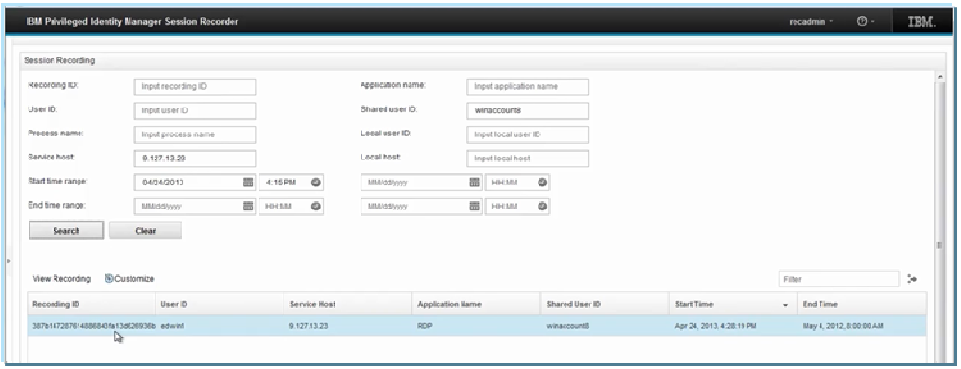
Admin ID

ISPIM Credential Vault

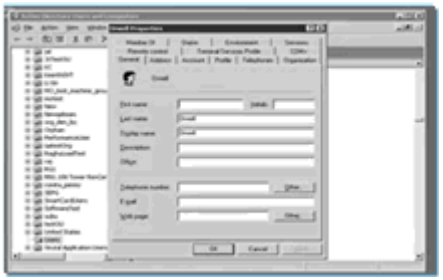


2 **Felvétel** (privileged user)

3 **Felvételek keresése, Visszajátszás kiválasztása** (Auditor)

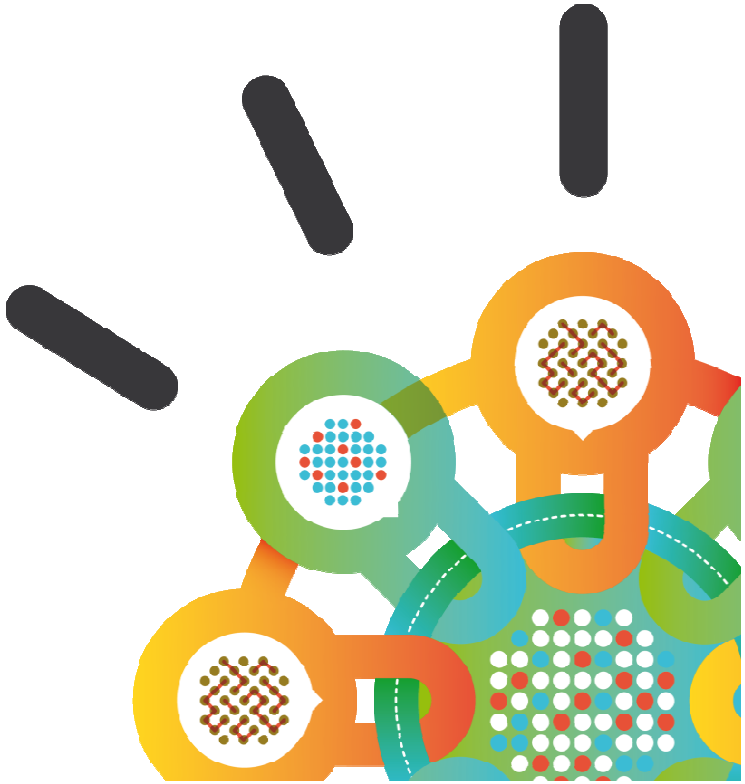


4 **Visszajátszás** (Auditor)



(alapértelmezetten szürkeárnyalatos felvétel)

© 2013 IBM Corporation

Security Intelligence.
Think Integrated.

Köszönöm a figyelmet!