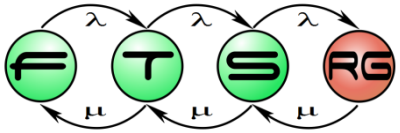
Infrastruktúra-felderítés és konfigurációmenedzsment-adatbázisok

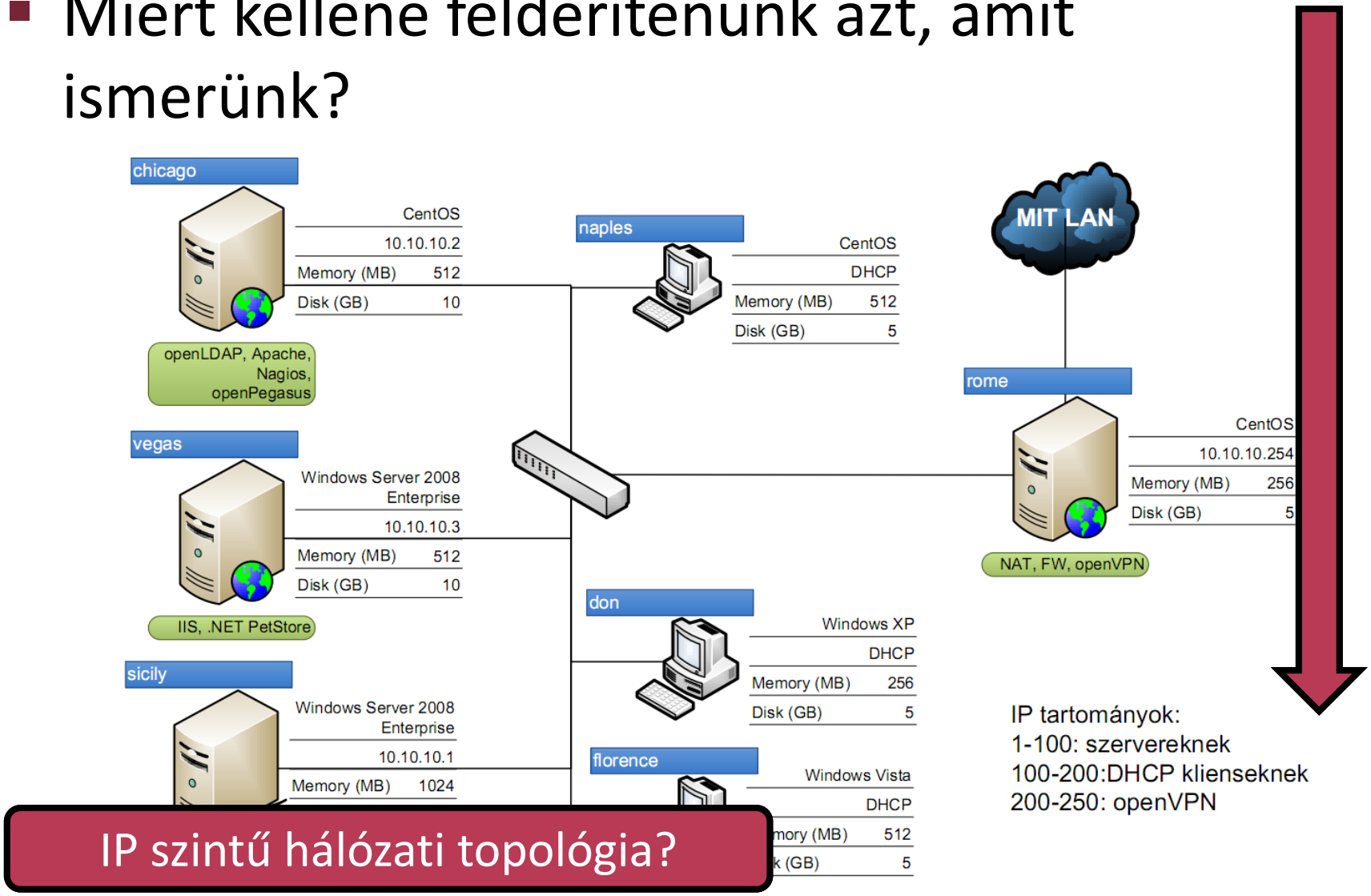
Kocsis Imre, Szombath István

http://mit.bme.hu/~ikocsis



Infrastruktúra-felderítés: motiváció

- Miért kellene felderítenünk azt, amit ismerünk?

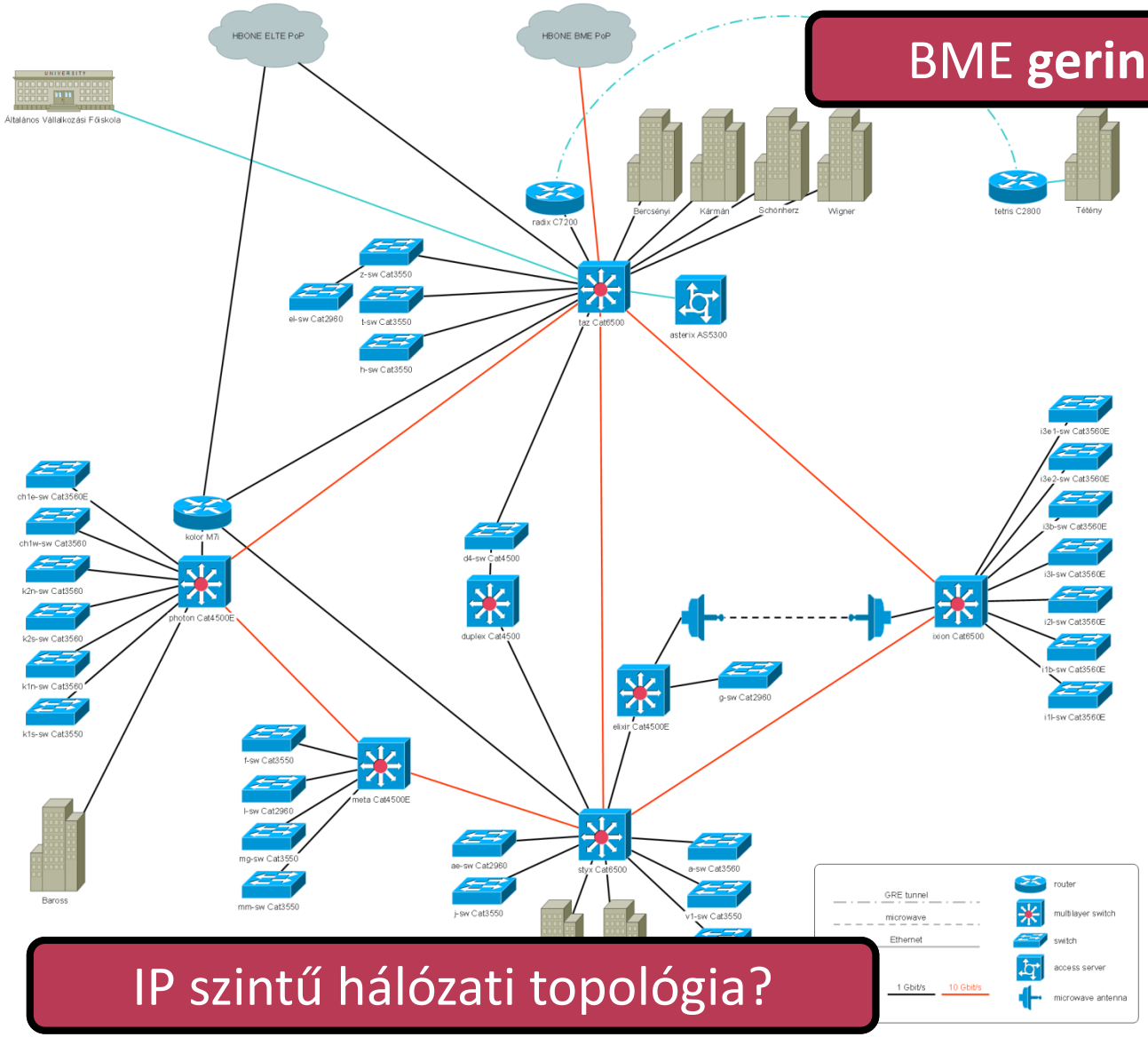


IP szintű hálózati topológia?

Infrastruktúra-felderítés: motiváció

IP szintű hálózati topológia?

Infrastruktúra-felderítés: motiváció



IP szintű hálózati topológia?

Mihez kell a pontos rendszerkép?

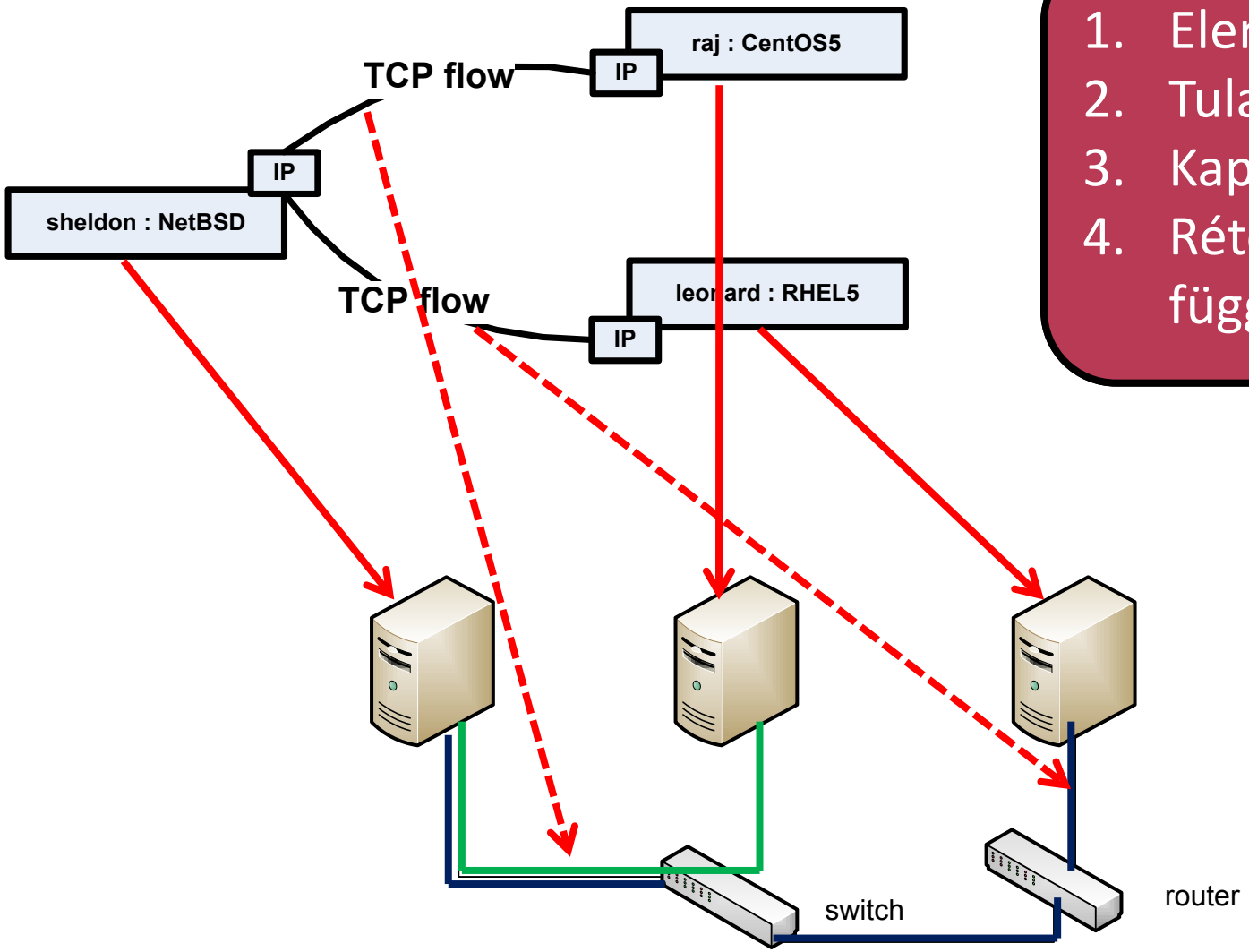
- „Eszközök” (assets) leltárazása
  - Hardvertől a licenszig
- Megfelelőségi (compliance) vizsgálatok
  - Törvényi szabályozástól a belső eljárásrendig
- Hibaok-keresés
- Hatásanalízis
  - Lásd ITIL változáskezelés
- …

Infrastruktúra-felderítés: miért?

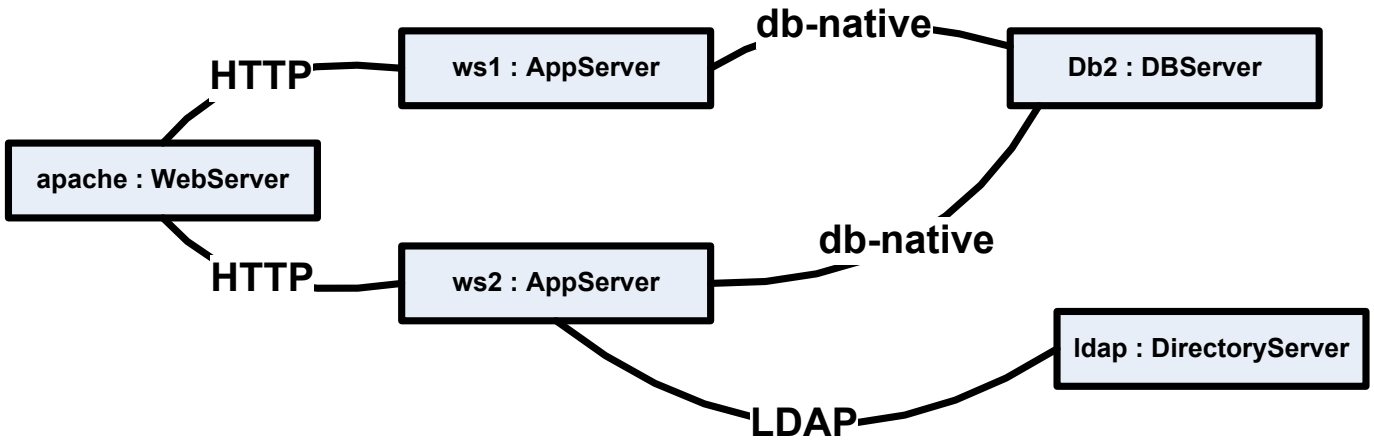
- Elavult dokumentáció, felejtés, kommunikáció hiánya, …
- Folyamatokat megkerülő változások
  - Jószándékú változtatásoktól a munkahelyi magánszerverig és tovább
  - N.B.: ha van egyáltalán változáskezelés…
- Rendszerek integrálása
- Infrastrukturális elemek logikai kapcsolatai
  - „Előre” jó modell: nehéz; zárt, menedzselt esetben is
  - Nem engedélyezett kapcsolatok?
- …

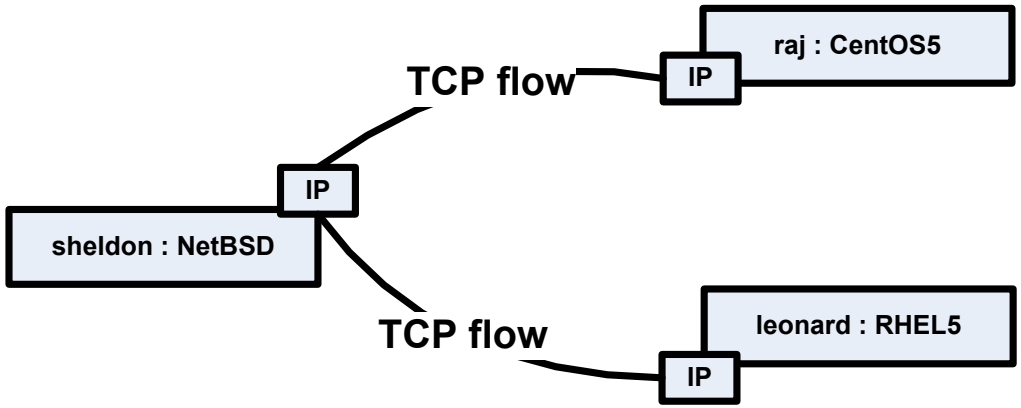
Infrastruktúra-felderítés: rétegek

1. Elemek
2. Tulajdonságaik
3. Kapcsolataik
4. Rétegek közötti függőségek

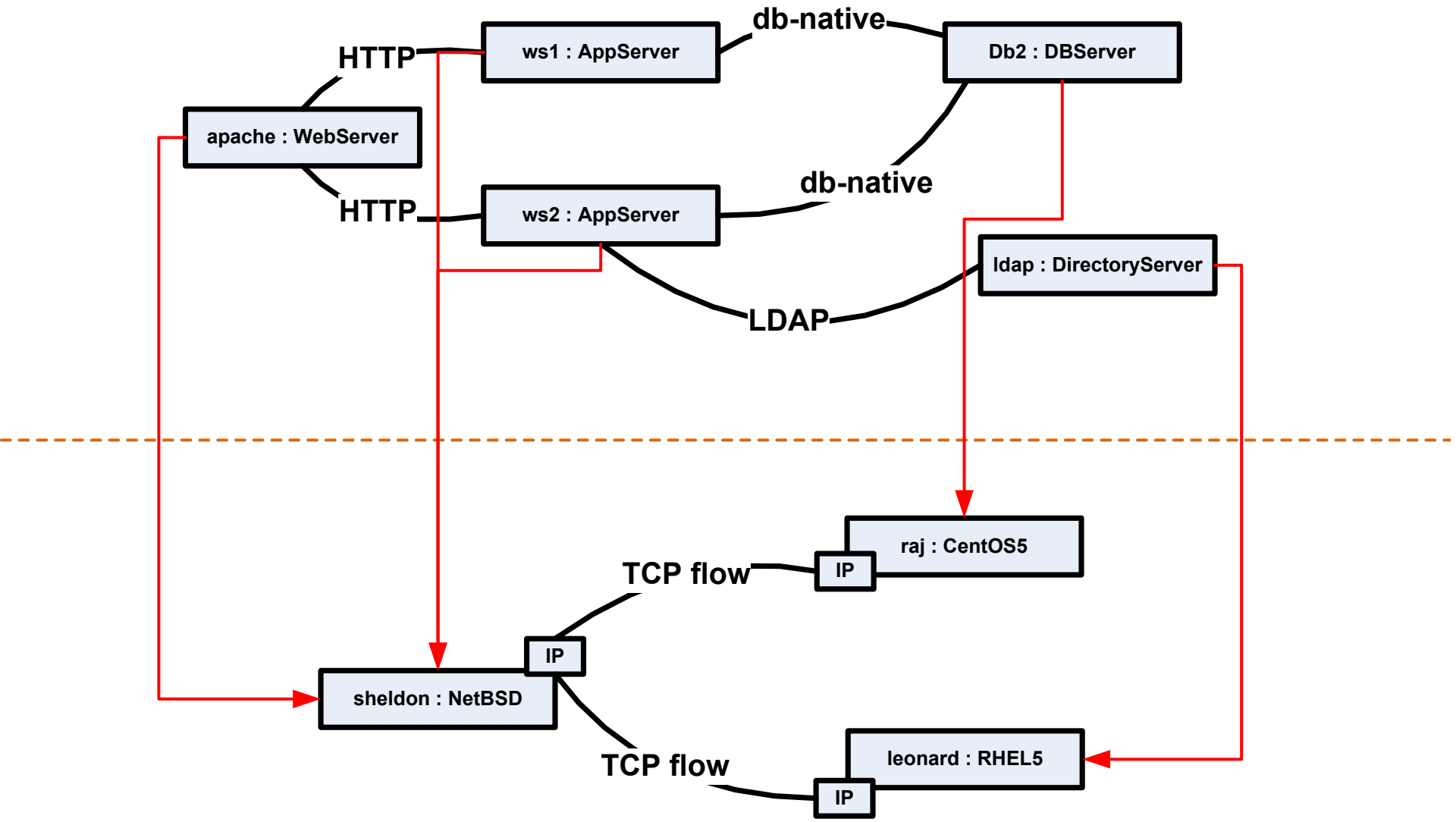


Infrastruktúra-felderítés: rétegek

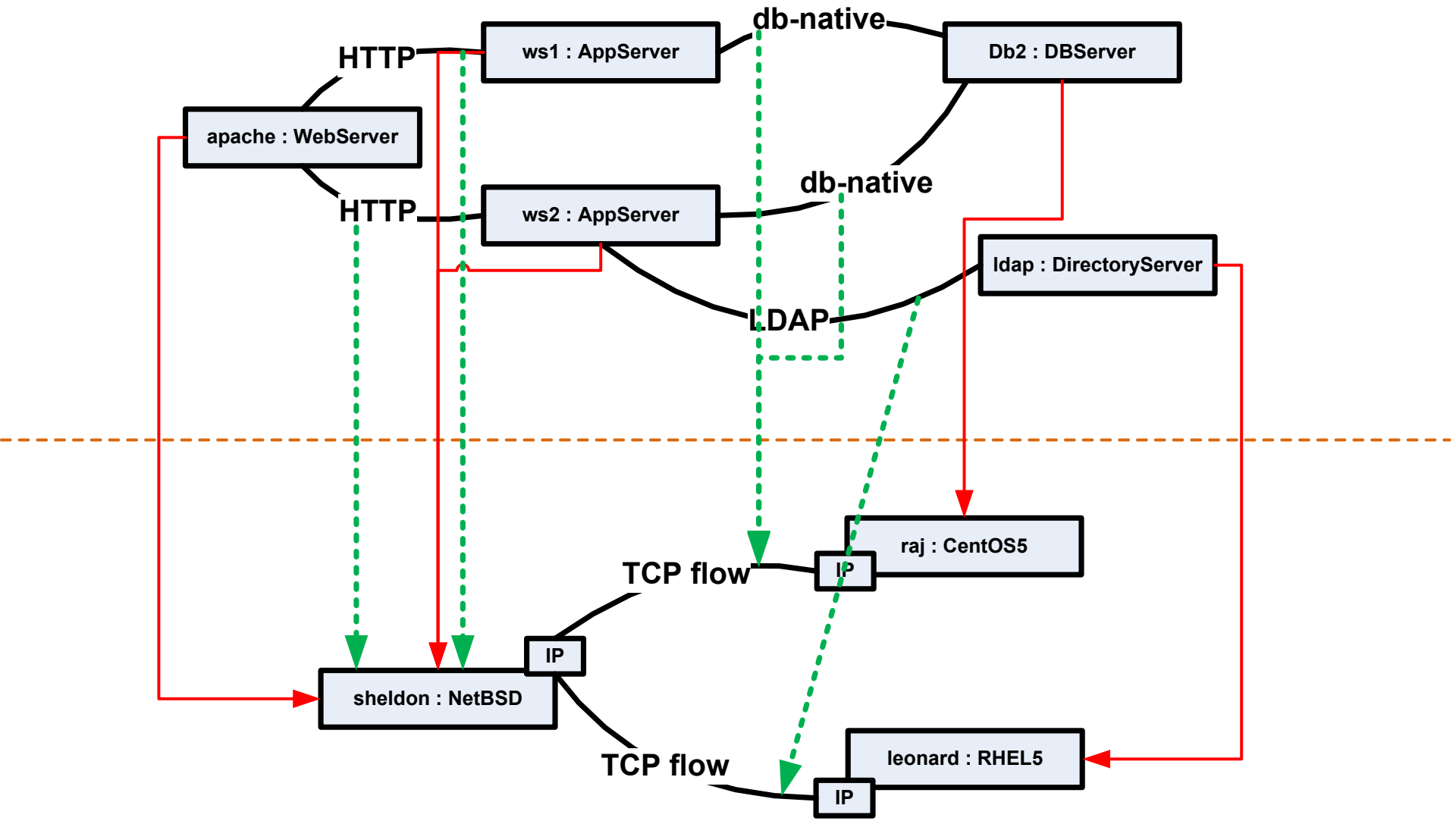




Infrastruktúra-felderítés: aspektusok



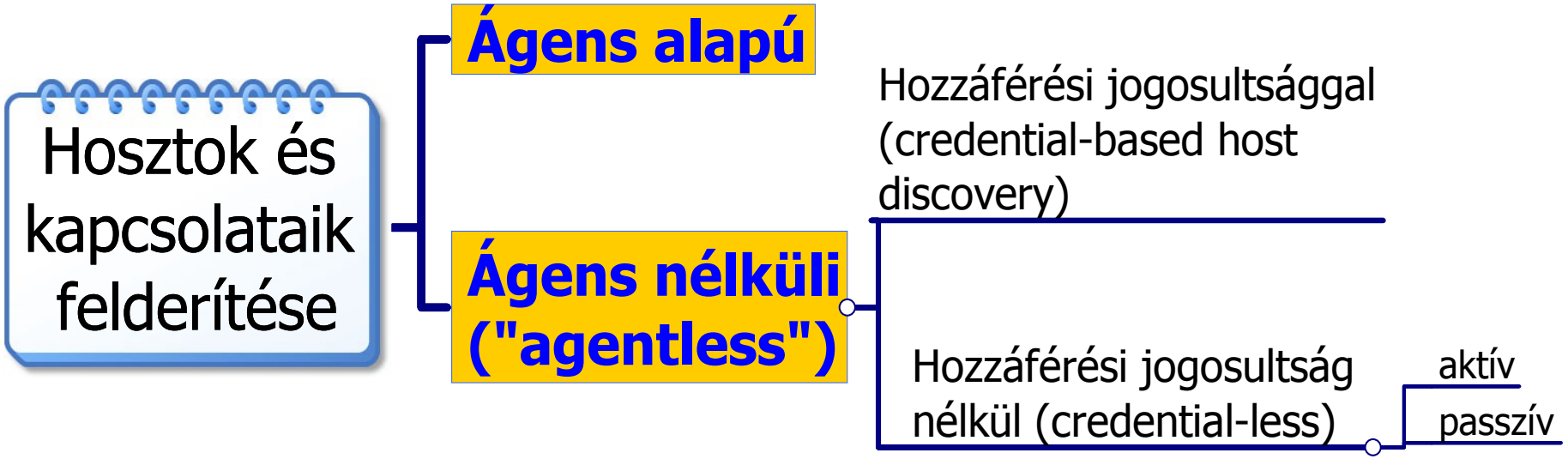
Infrastruktúra-felderítés: aspektusok



Tanulságok

- A kapcsolatok felderítése valódi feladat
- „Rétegek” és kapcsolataik: komoly modellezési vetület
  - Sorvezető: CIM
  - Rétegeket összekapcsoló logika?
- Támogató eszközök és automatizáció kell

Taxonómia


Hosztok és kapcsolataik felderítése
Ágens alapú
Ágens nélküli ("agentless")
Hozzáférési jogosultsággal (credential-based host discovery)
Hozzáférési jogosultság nélkül (credential-less)
aktív
passzív

Felderítés

- Ágens alapú
  - Értelemszerűen: ágens
  - Erőforrások?
  - Eseményvezérelt is lehet
- Hozzáférési jogosultságokkal
  - WMI, SNMP, ssh (+ expect) + $foo, …
    - Akkor mitől „ágens nélküli”?
  - Biztonsági rés / jelszavak karbantartása

Felderítés – „credential-less”, aktív

- intruzív, támadásokra hasonlít
  - szűrések/tiltások! – nem mintha lenne tapasztalatunk ☺
- „felületi” információk
  - azt azért feltételezhetjük, hogy nem Metasploit a következő lépés…
- ARP scan, ping sweep, port scan, TCP/IP stack (OS) fingerprinting, service fingerprinting, …
- nmap

Felderítés – „credential-less”, passzív (3)

- hálózati forgalom „lehallgatása”
  - Wireshark
  - Mély protokoll-analízis (deep inspection)
  - Kapcsolt Etherneten?

- hálózati elemeken belüli forgalom-megfigyelés
  - IP szint: NetFlow
    - szabvány: IP Flow Information eXport, IPFIX (RFC5101/5102)
  - Klasszikusan egy „flow” ~:
    {source | dest}, {IP | port}, ingress if, IP ToS
  - Router: flow record-okat ad ki
  - „Deep (packet) inspection” is létezik

nmap


open ssh
exact OS matches for host
map run completed -- 1 IP address (1 host up) scanneds
sshnuke 10.2.2.2 -rootpw="Z1ON0101"
nnecting to 10.2.2.2:ssh ... successful.
tempting to exploit SSHv1 CRC32 ... successful.
seting root password to "Z1ON0101".
sten open: Access Level <9>
sh 10.2.2.2 -l root
t@10.2.2.2's password:
enter password

Demo nmap

- nmap GUI
- scan
  - Windows → stock Ubuntu
  - Windows → Ubuntu + Apache
  - Ubuntu → Windows with FW
  - Ubuntu → Windows w/o FW

- **Idegen hálózatban/eszközökön támadásnak minősül!**

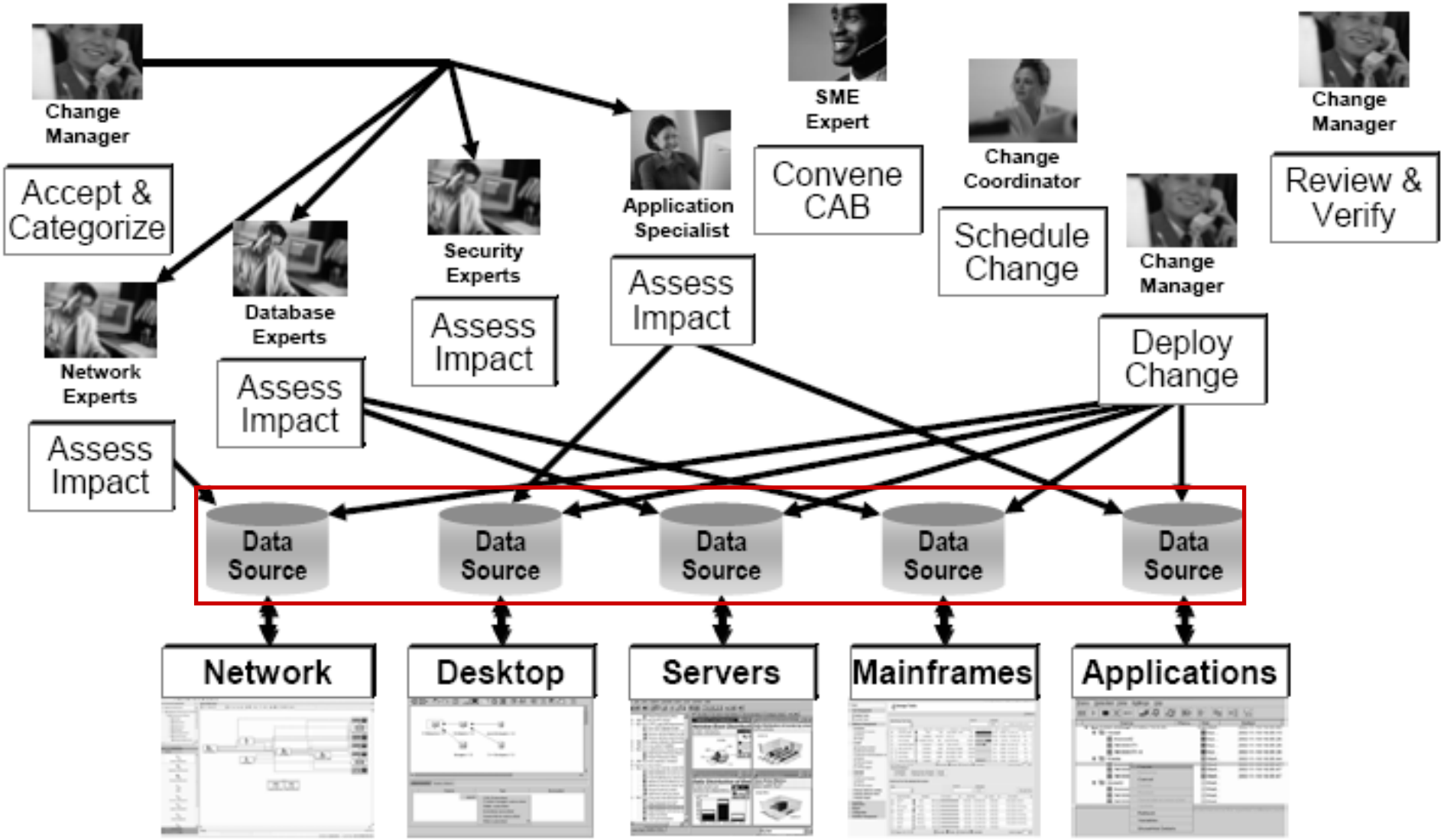
Központi konfiguráció-menedzsment adatbázis

- Hol tároljuk az adatokat?
  - Hálózatmenedzsment eszköz
  - Szoftverterítő és –karbantartó megoldás
  - Hardver leltár
  - Licenszkövető rendszer
  - Szolgáltatási szint menedzsment rendszer
  - …
- Így viszont:
  - Nincsenek „menedzsment silók” közötti relációk
  - Tipikus IT menedzsment folyamatok: több forrásból adat

Linux/UNIX hosztbázisú felderítés

- SNMP/CIMOM/Advanced Package Tool/…:
  - Igen sok terület valójában jól lefedett
- Problematikus terület: folyamatok/szolgáltatások belső függőségei (IPC!)
  - File
  - Signal
  - Socket
  - Message queue
  - Pipe
  - Shared memory
  - …
- Problematikus terület: távoli „kliens” és „szerver” összekapcsolása
  - TCP szintig: lsof, netstat, …

Központi konfiguráció-menedzsment adatbázis



Konfigurációs elemek (ITIL v3)

- A *konfigurációs elemek* (*Configuration Item*, *CI*) olyan (rendszer)komponensek, melyek menedzselése szükséges valamely IT szolgáltatás nyújtásához. *[…]*

- Tipikusan CI-ként kezelt rendszerelemek:
  - IT szolgáltatások
  - Hardver, szoftver
  - Épületek, emberi erőforrások
  - Formális dokumentáció (folyamatok, SLA-k)
  - Folyamat-adatok (incidensek, problémák)

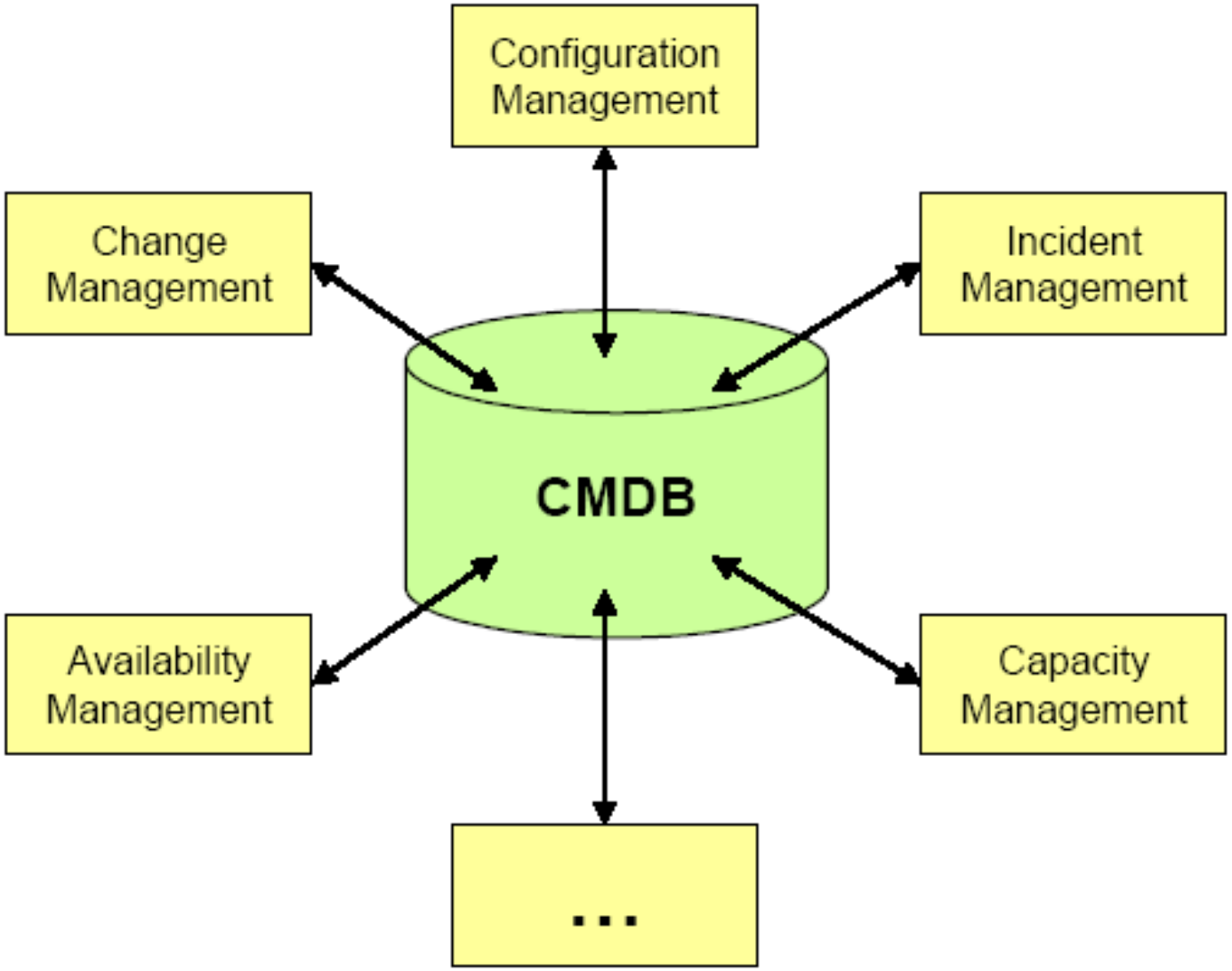
CMDB (ITIL v3)

- *Központosított* „adatbázis” ami *CI*-k *attribútumait* és azok más CI-kkel való *kapcsolatait* tárolja.

- Megjegyzések
  - az ITIL alapvetően még mindig folyamat-gyűjtemény
  - A definíció inkább funkcionális igény, mint specifikáció
  - Általában relációs vagy OO technológia

Figyelem: ez egy egyszerűsített definíció
(kimaradt pl. : CMS, CR, életciklus)

ITIL CMDB


Configuration Management
Change Management
Incident Management
CMDB
Availability Management
Capacity Management
...

Általános követelmények (Gartner)

Federation – adatbázisok federációja

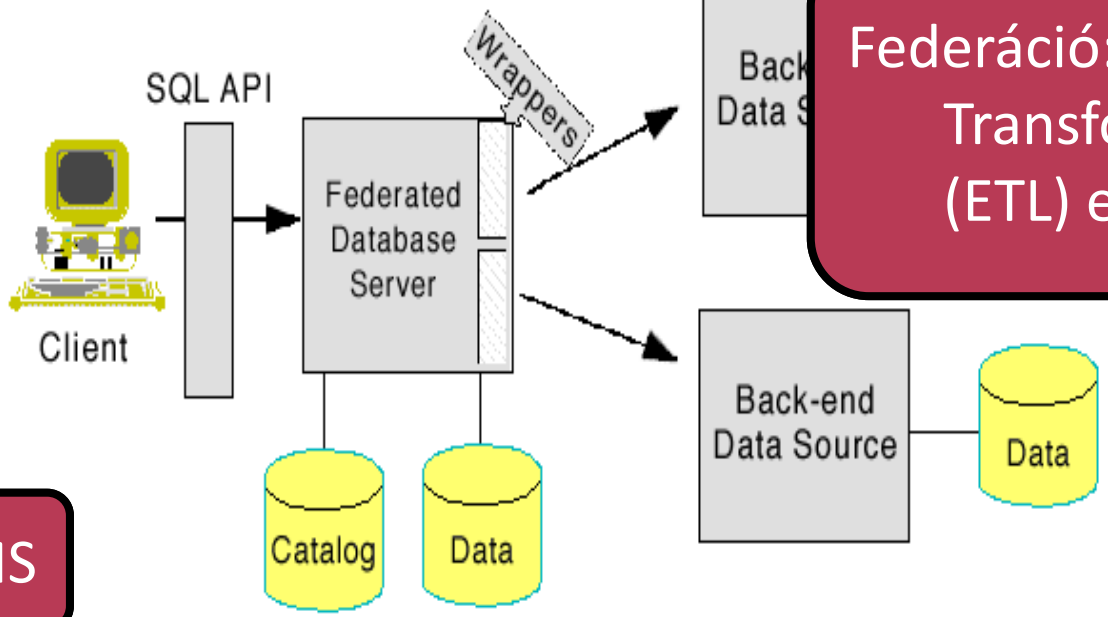
Reconciliation – adatforrások „kibékítése” (adategyeztetés)

Synchronization – szinkronizáció

Mapping and Visualization – leképezés és vizualizáció

Federáció

- Federált CMDB
  - „*Management Data Repository*”-k (*MDR*) kombinációja
  - legalább egy federálja a többit
  - menedzsment adatok aggregált nézete

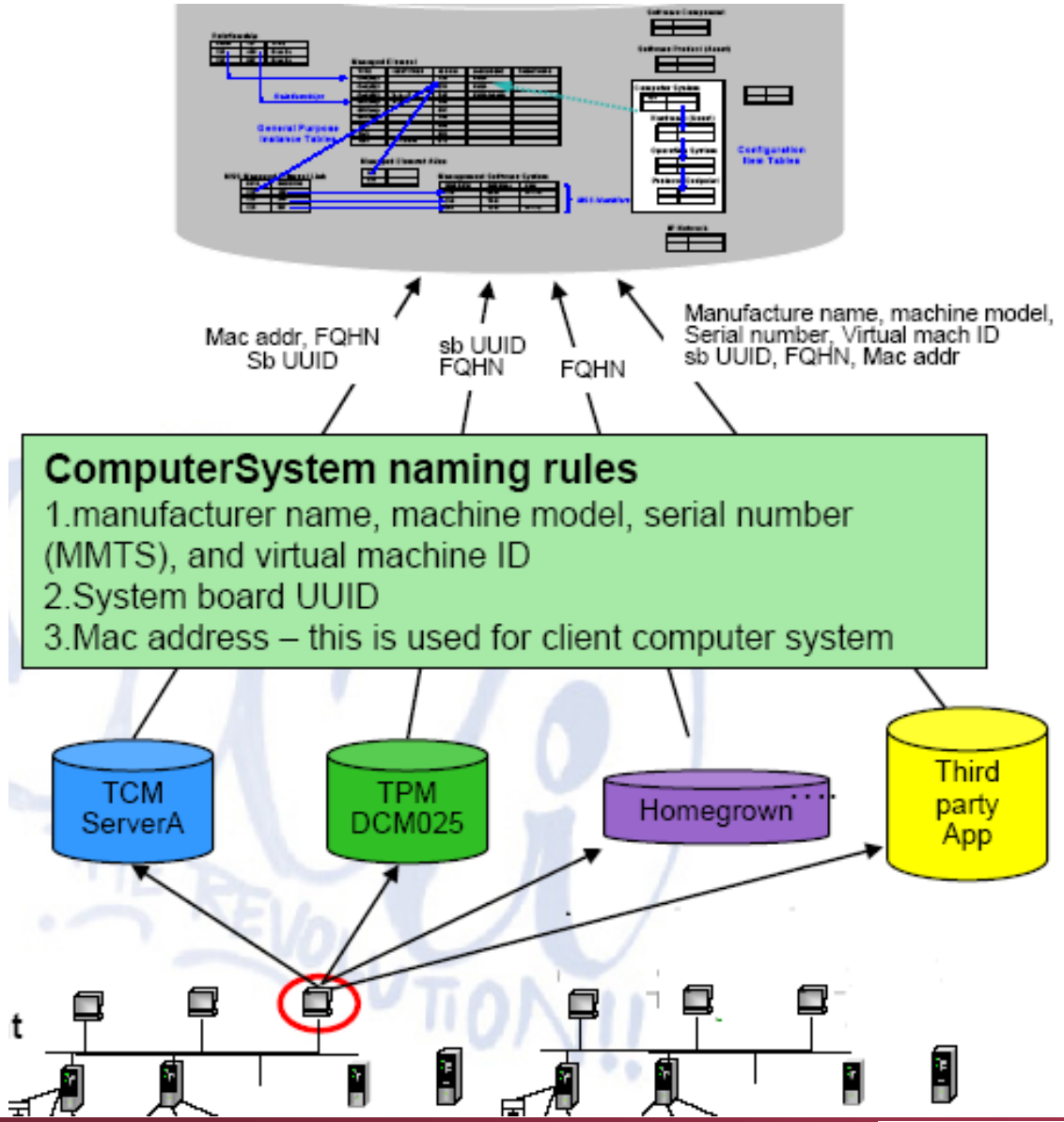


Federáció: az „Extract-Transform-Load” (ETL) ellentéte

meta-DBMS

Adategyeztetés

- Alapprobléma: ugyanazon CI más névvel / ID-val a különböző adatforrásokban
- Konfigurációs elem integritásának megőrzése
- Új összefüggések létrehozása
- Erősen gyártóspecifikus



Termékek

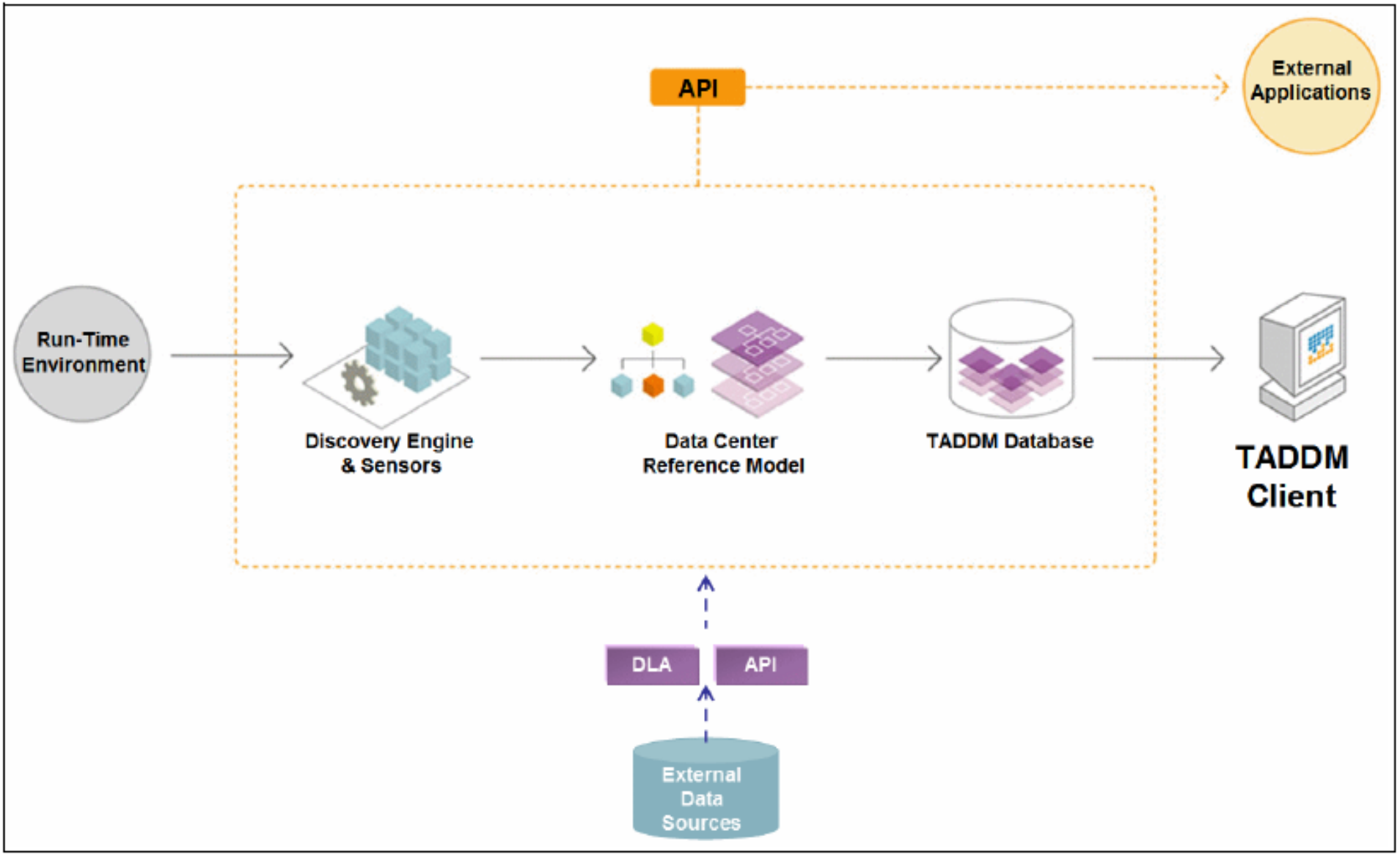
- IBM Tivoli Application Dependency Discovery Manager (TADDM)
  - Adatmodell alapja: CIM
- HP Universal CMDB
- BMC Atrium CMDB
- Jónéhány kisebb/FOSS megoldás

- Federáció nem jellemző
- Integrált felderítő-képességek
- Periodikus, teljes felderítés

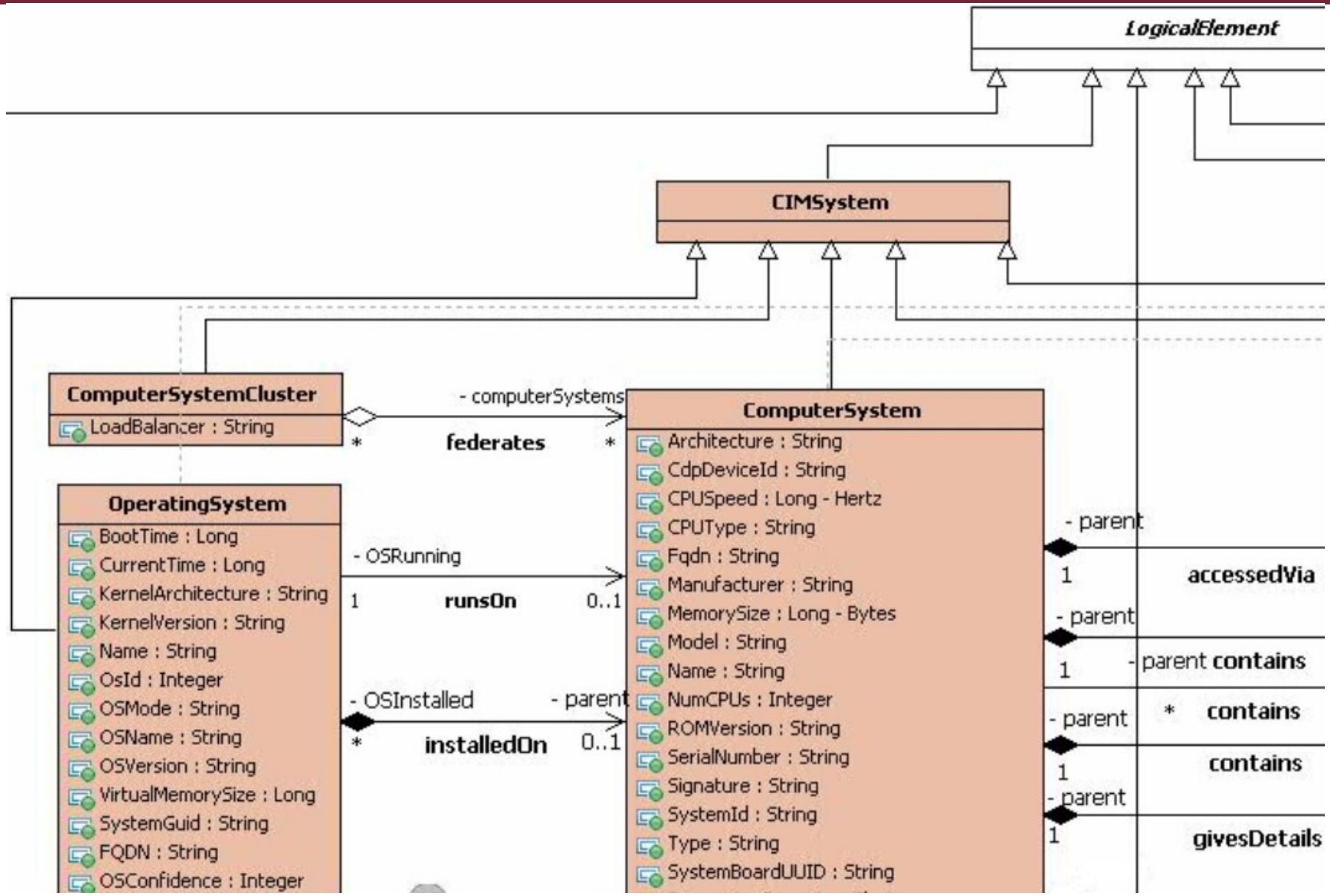
IBM Tivoli Application Dependency Discovery Manager (TADDM)

- IBM CMDB megvalósítása
- Fejlett IT infrastruktúra felderítés, követés, tárolás, …
  - Szenzorok, adapterek, ágensek,…
  - ITIL folyamatok támogatása
- Automatizálható
- Központosított
- Szabványos adattárolás, integrációs lehetőségek
- Nagyvállalati rendszerekre optimalizált
- http://www-01.ibm.com/software/tivoli/products/taddm/
- http://www.redbooks.ibm.com/abstracts/sg247222.html?Open

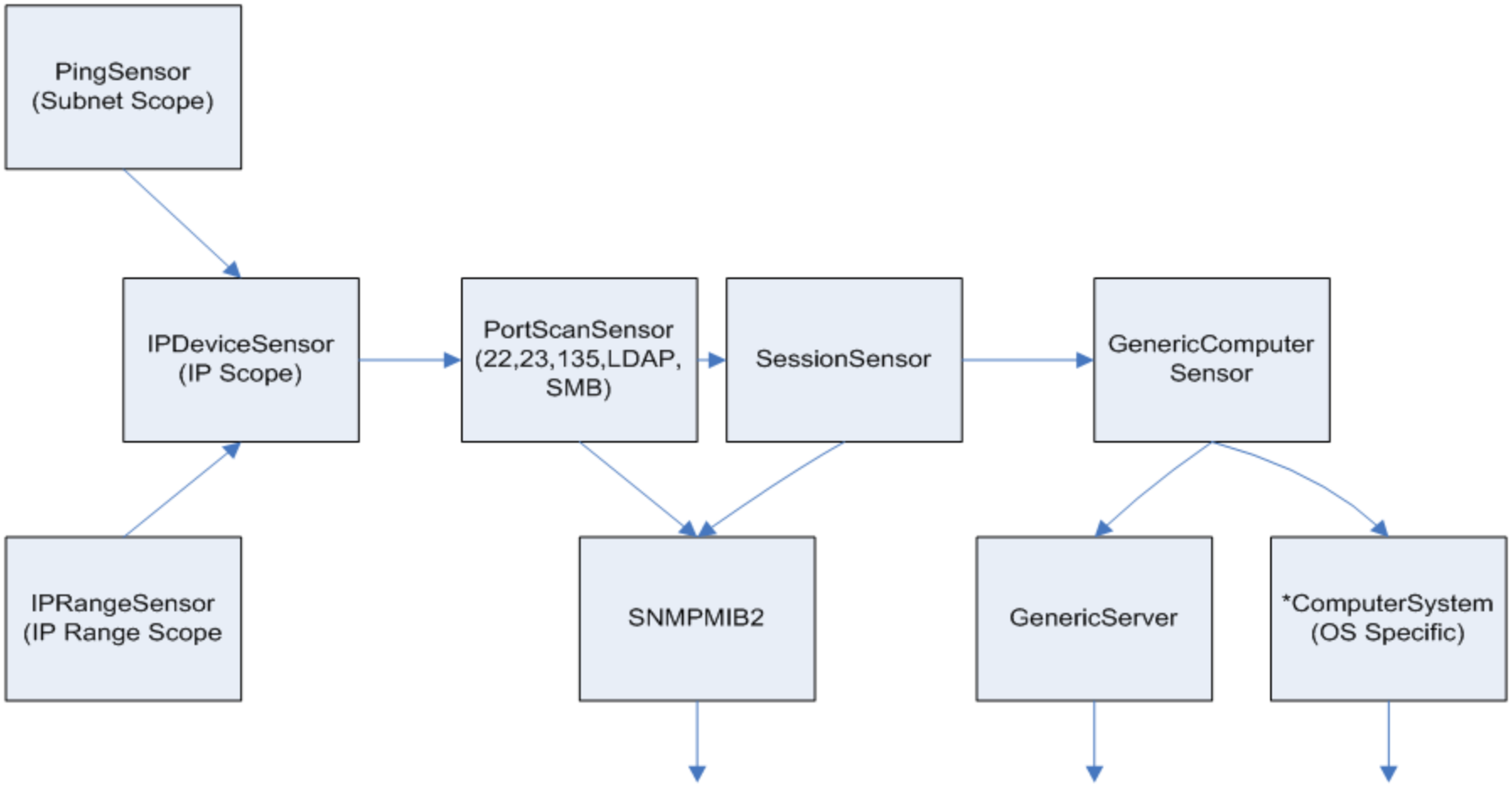
Architektúra és Integráció



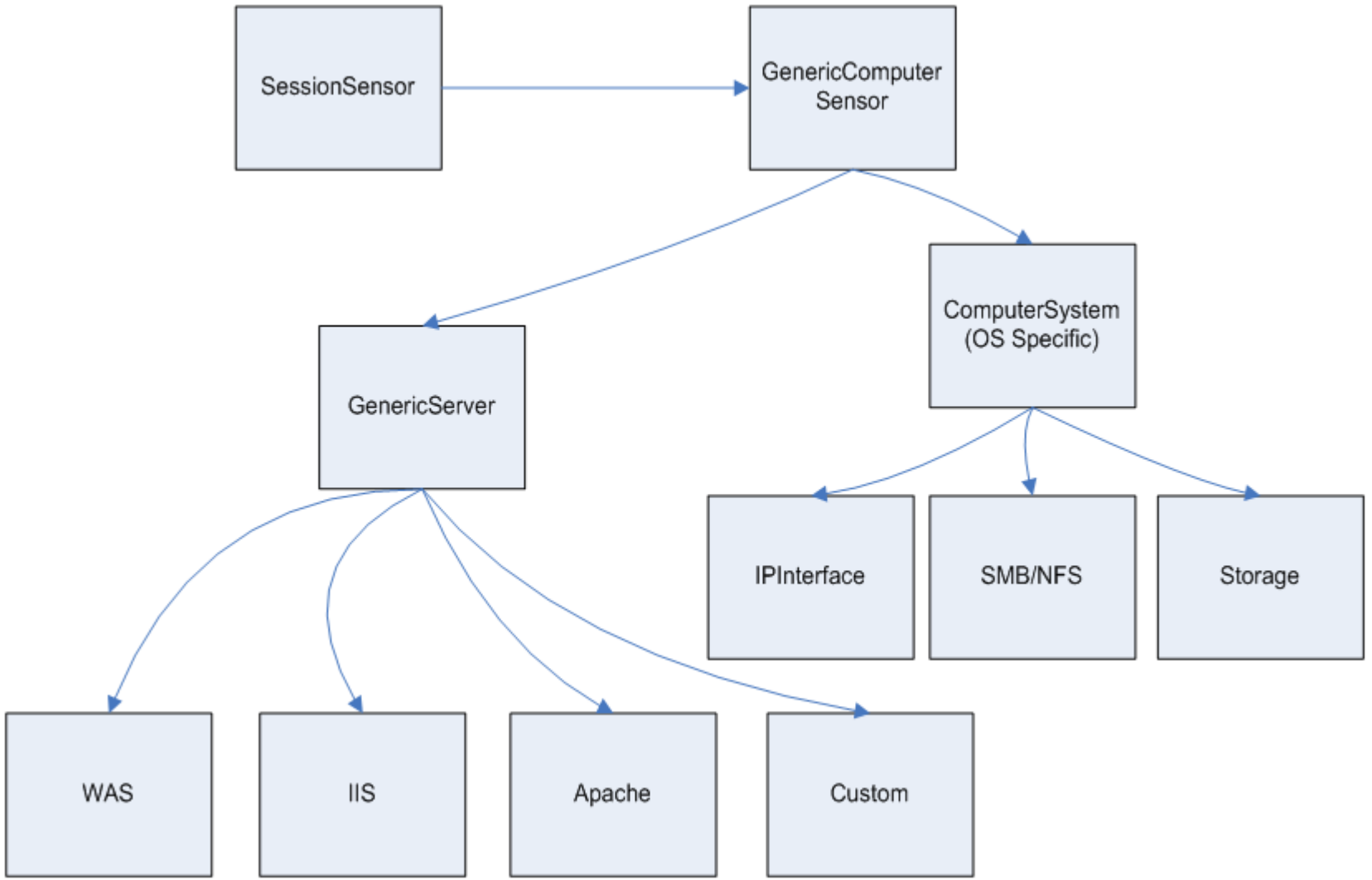
Adatmodell (részlet…)



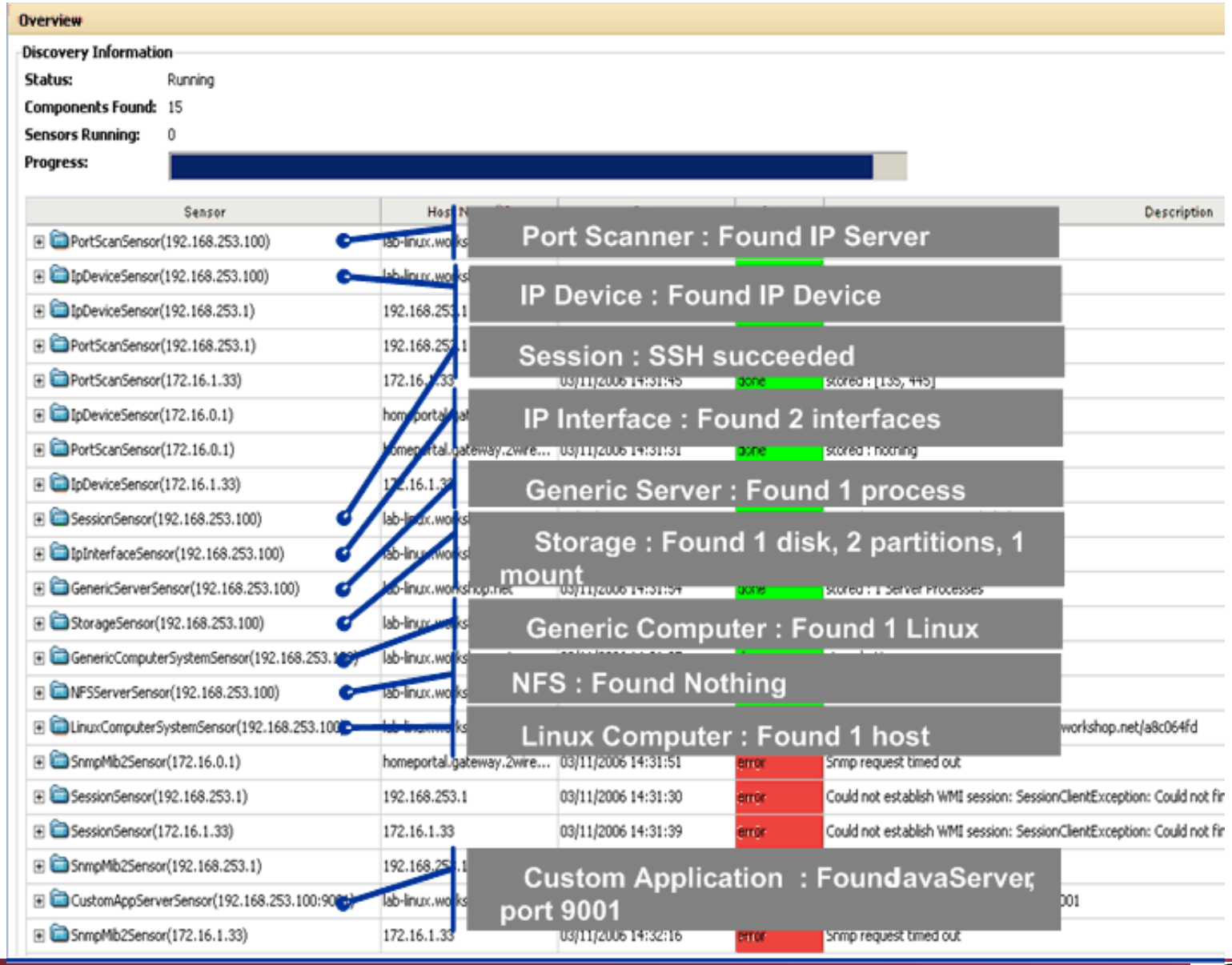
Automatizált felderítés – kaszkád-logika

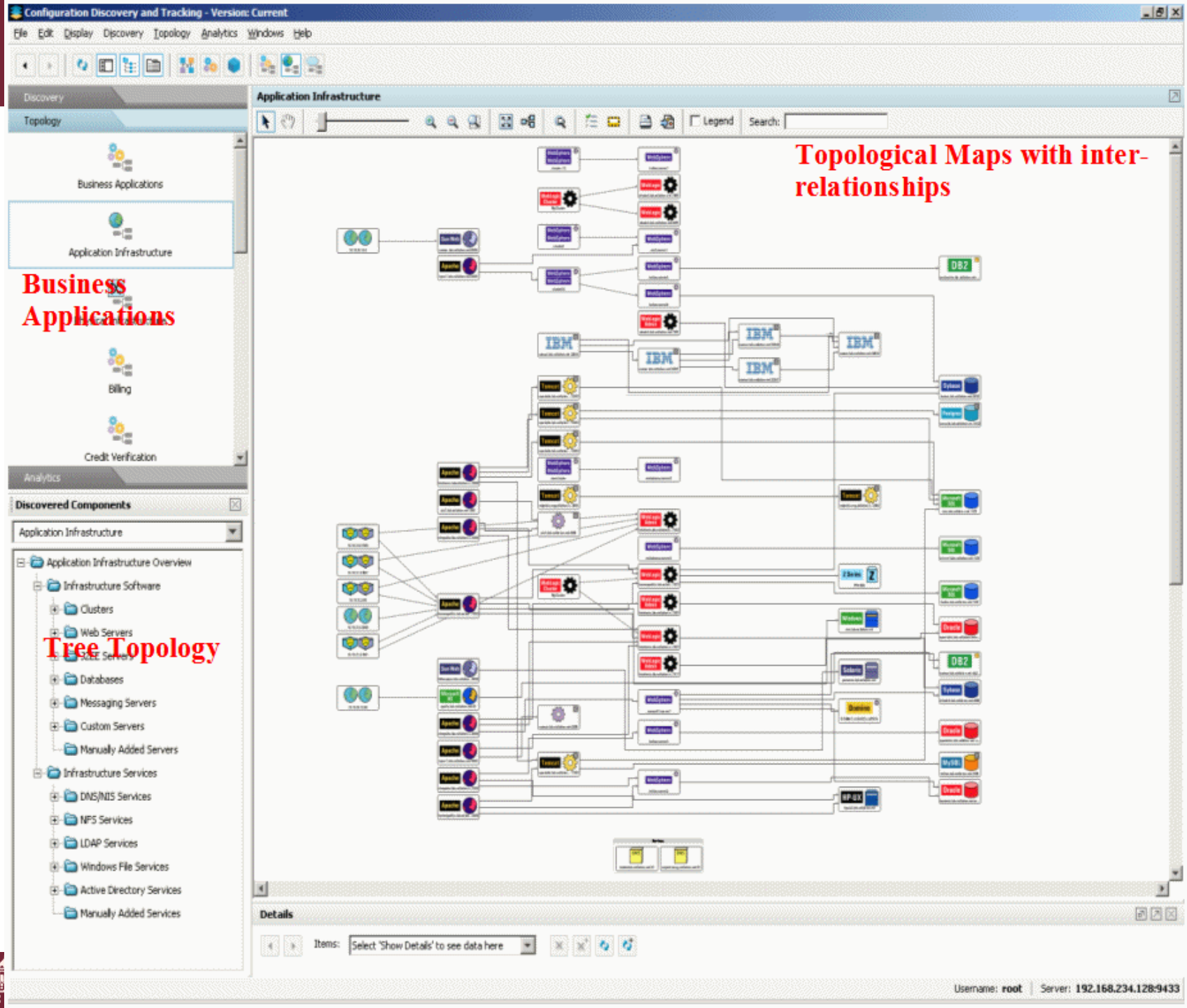


Automatizált felderítés – kaszkád-logika



Felderítés


Overview
Discovery Information
Status: Running
Components Found: 15
Sensors Running: 0
Progress:
Sensor
Description
PortScanSensor(192.168.253.100)
IpDeviceSensor(192.168.253.100)
IpDeviceSensor(192.168.253.1)
PortScanSensor(192.168.253.1)
PortScanSensor(172.16.1.33)
IpDeviceSensor(172.16.0.1)
PortScanSensor(172.16.0.1)
IpDeviceSensor(172.16.1.33)
SessionSensor(192.168.253.100)
IpInterfaceSensor(192.168.253.100)
GenericServerSensor(192.168.253.100)
StorageSensor(192.168.253.100)
GenericComputerSystemSensor(192.168.253.
NFSServerSensor(192.168.253.100)
LinuxComputerSystemSensor(192.168.253.10
SnmpMib2Sensor(172.16.0.1)
SessionSensor(192.168.253.1)
SessionSensor(172.16.1.33)
SnmpMib2Sensor(192.168.253.1)
CustomAppServerSensor(192.168.253.100:90
SnmpMib2Sensor(172.16.1.33)
homeportal.gateway.2wire...
03/11/2006 14:31:51
Snmp request timed out
192.168.253.1
03/11/2006 14:31:30
Could not establish WMI session: SessionClientException: Could not fir
172.16.1.33
03/11/2006 14:31:39
Could not establish WMI session: SessionClientException: Could not fir
Port Scanner : Found IP Server
IP Device : Found IP Device
Session : SSH succeeded
IP Interface : Found 2 interfaces
Generic Server : Found 1 process
Storage : Found 1 disk, 2 partitions, 1 mount
Generic Computer : Found 1 Linux
NFS : Found Nothing
Linux Computer : Found 1 host
Custom Application : FoundJavaServer, port 9001


Configuration Discovery and Tracking - Version: Current
File Edit Display Discovery Topology Analytics Windows Help
Discovery
Topology
Business Applications
Application Infrastructure
Billing
Credit Verification
Analytics
Discovered Components
Application Infrastructure
Application Infrastructure Overview
Infrastructure Software
Clusters
Web Servers
Databases
Messaging Servers
Custom Servers
Manually Added Servers
Infrastructure Services
DNS/NIS Services
NFS Services
LDAP Services
Windows File Services
Active Directory Services
Manually Added Services
Application Infrastructure
Legend
Search:
Topological Maps with inter-relationships
Business Applications
Tree Topology
Details
Items:
Select 'Show Details' to see data here
Username: root
Server: 192.168.234.128:9433

Configuration Discovery and Tracking - Version: Current

File Edit Display Discovery Topology Analytics Windows Help

Discovery

Topology

Business Applications

Application Infrastructure

Physical Infrastructure

myBusinessApp

Analytics

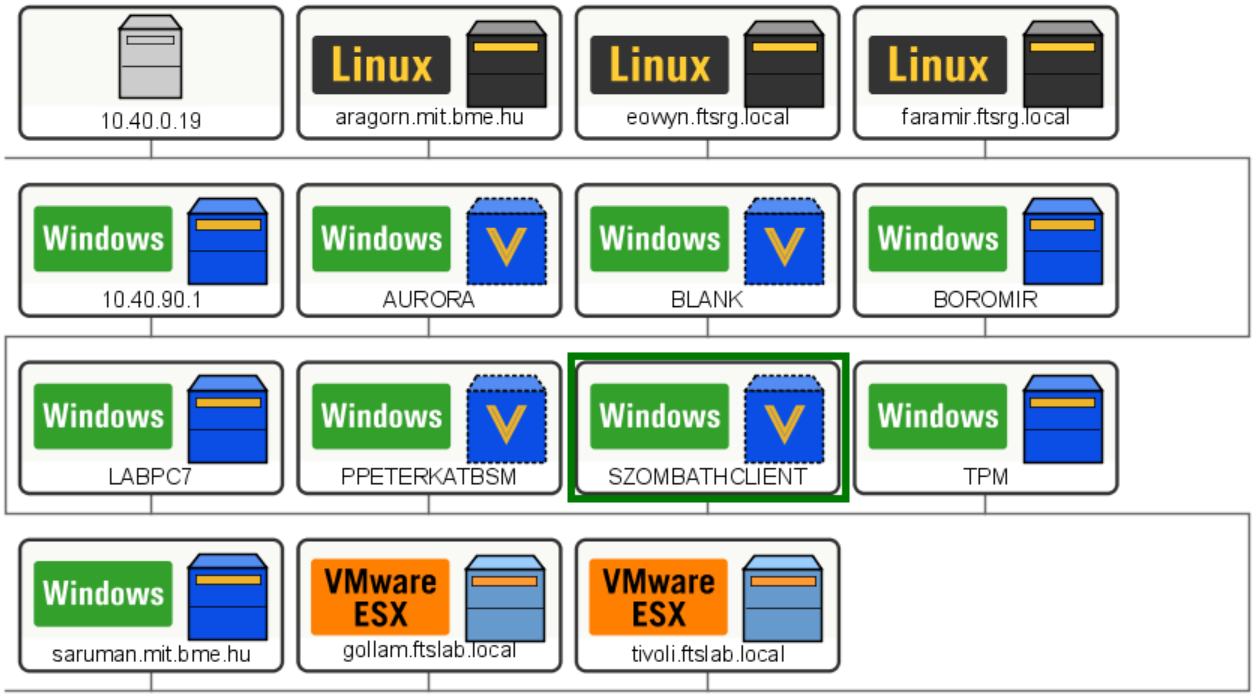
Discovered Components

Application Infrastructure

- OracleAppServer
- mySAP
- Other J2EE Servers
  - Tomcat(4)
    - sauron.mit.bme.hu:8005
    - sauron.mit.bme.hu:8005
    - sauron.mit.bme.hu:8005
    - sauron.mit.bme.hu:8005
- Manually Added J2EE Servers
- SMS
- Citrix
- Databases
  - Oracle
  - Sybase
  - Microsoft SQL Server
  - DB2(3)
    - :idsldap
    - eowyn.ftsrg.local:db2inst1

Subnet - 10.40.0.0/16

Legend Search:



Details

Items: SZOMBATHCLIENT

General | Router Details | OS | Devices | Storage | IP | Interfaces | Software Components | Services

Name:	szombath_client
Fully qualified domain name:	SZOMBATHCLIENT
Object Type:	Windows Computer System
Last Modified Time:	6/22/07 12:01 CET
Manufacturer:	VMware, Inc.
Model:	VMware Virtual Platform

Username: **administrator** | Server: **eowyn.ftslab.local:9433**