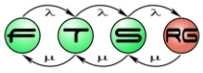
Intelligens rendszerfelügyelet

Rendszermonitorozás

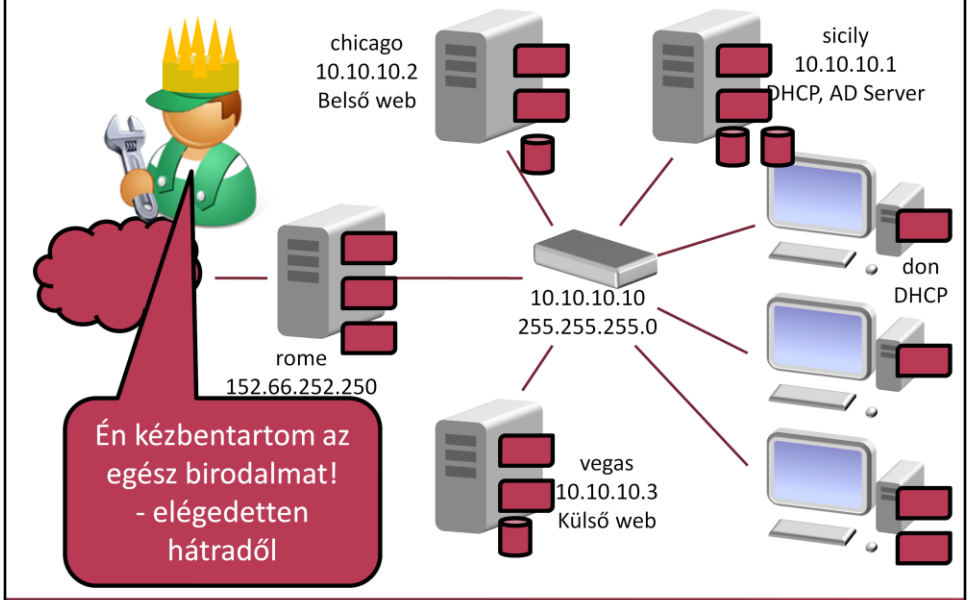
Tóth Dániel, Kocsis Imre



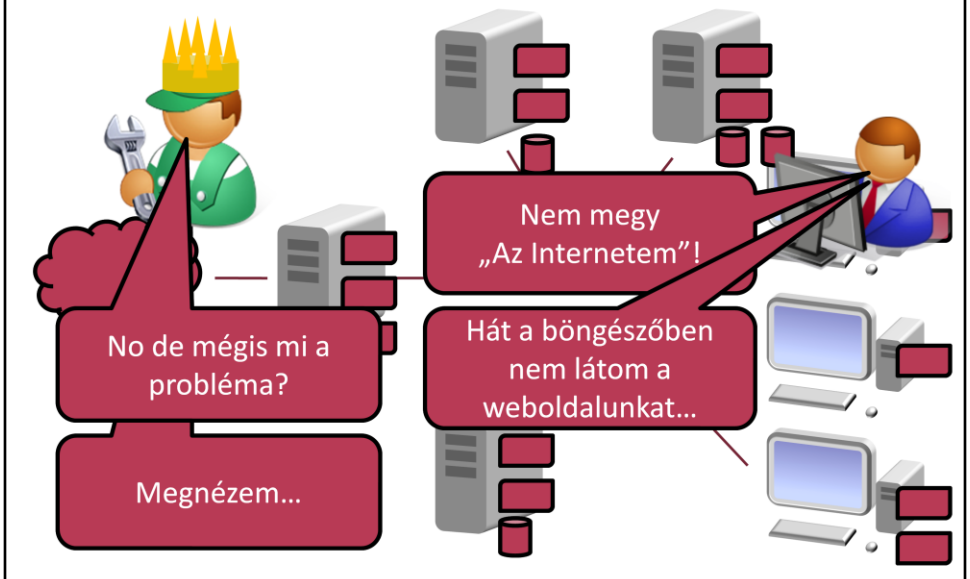
Budapesti Műszaki és Gazdaságtudományi Egyetem
Méréstechnika és Információs Rendszerek Tanszék

Utolsó módosítás: 2011. 04. 06.

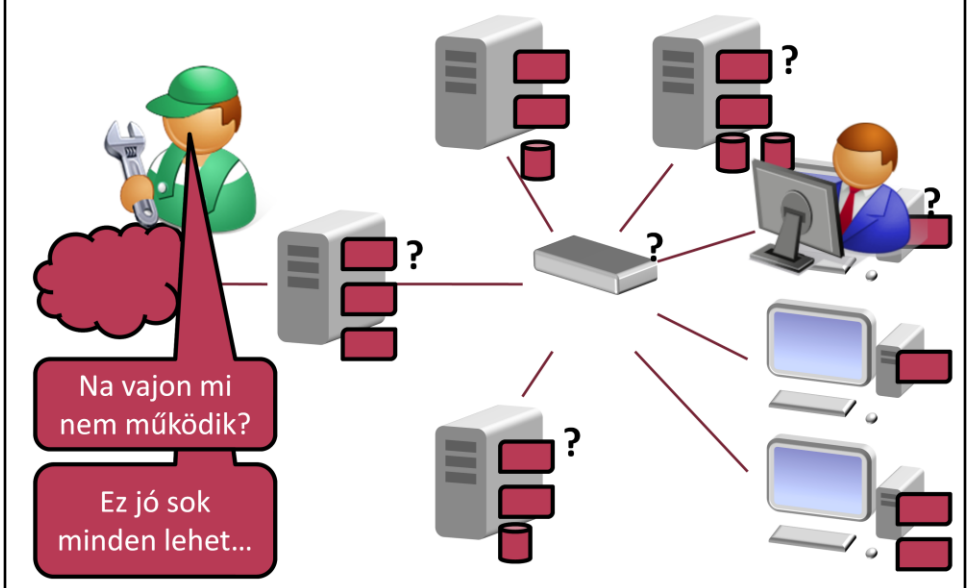
„Kézbentartott” rendszer



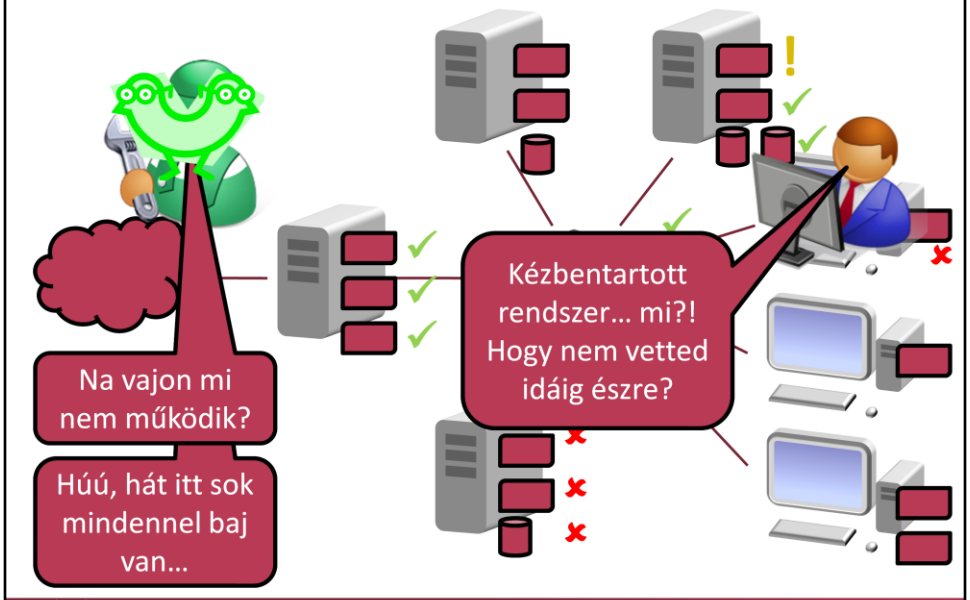
Káosz


Nem megy „Az Internetem”!
No de mégis mi a probléma?
Hát a böngészőben nem látom a weboldalunkat…
Megnézem…

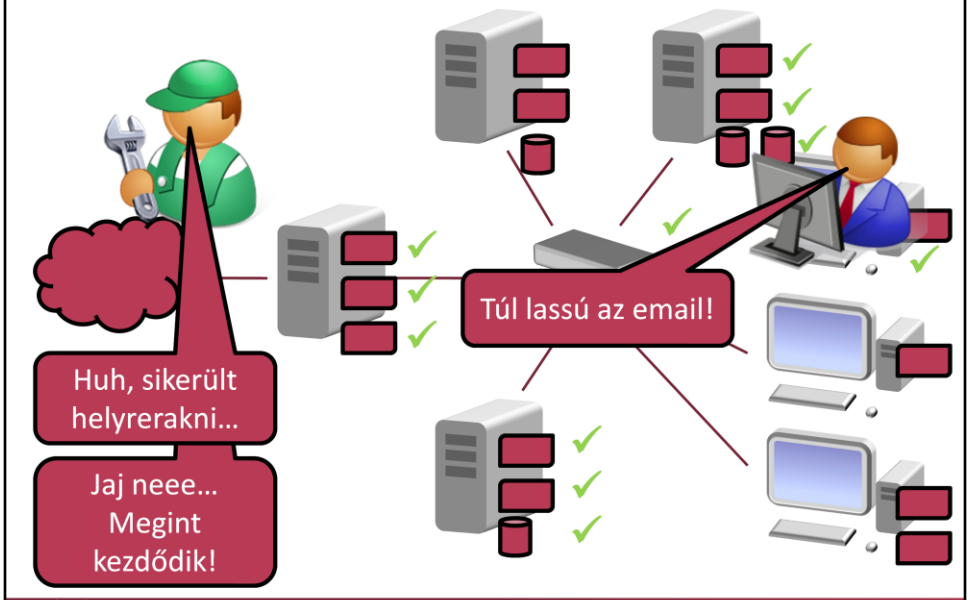
Káosz



Káosz


Na vajon mi nem működik?
Húú, hát itt sok mindennel baj van…
Kézbentartott rendszer… mi?! Hogy nem vetted idáig észre?

Káosz


Huh, sikerült helyrerakni…
Jaj neee… Megint kezdődik!
Túl lassú az email!

Táblánál Diagnosztikai alapfogalmak

- Hibadetektálás
- Hibalokalizáció

Rendszermonitorozás

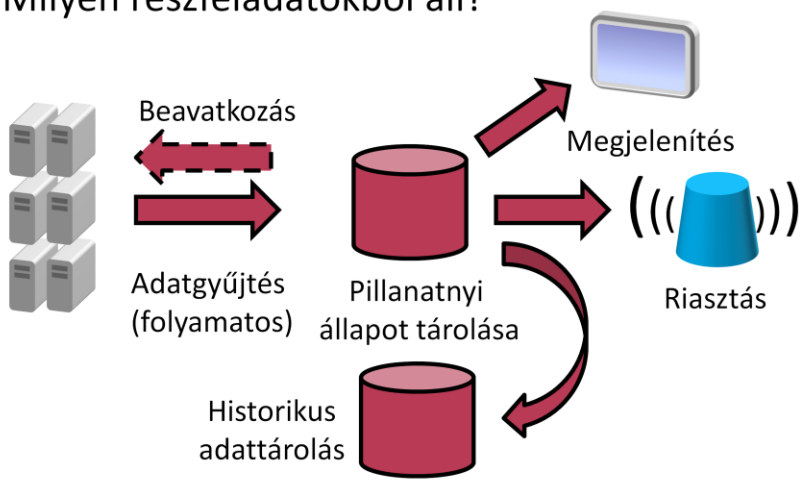
- A rendszer túl bonyolult
  - Ember nem látja át a teljes működését
  - Valami mindig történik benne…
  - Csak akkor értesülünk róla, ha a felhasználók nyaggatnak, hogy valami nem megy
    - ($$$!)
  - Csak akkor vesszük észre, hogy baj van, ha már tényleg nagy baj van (jó lett volna előbb preventív jelleggel)
  - A rendszer teljesítményéről, kihasználtságáról nincs elképzelésünk
    - Pedig ilyen adatok nélkül nehéz tervezni…

Rendszermonitorozás: állapotkép fenntartása

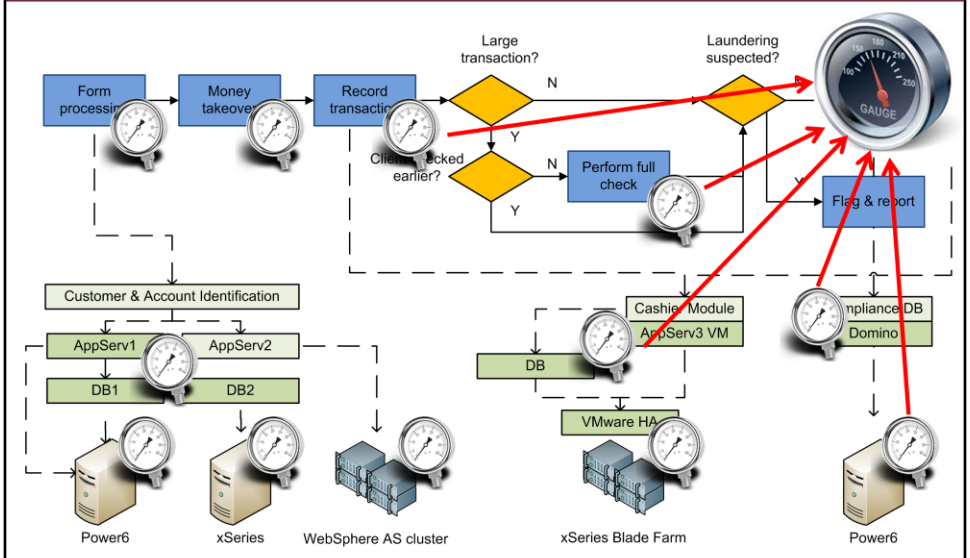
- Infrastrukturális komponensek és szolgáltatások működőképességéről
- Terhelésről, erőforrások kihasználtságáról
- Topológiáról, konfigurációról
  - Kapcsolat a konfiguráció-menedzsmenttel!
- Biztonságról

Rendszermonitorozás részei

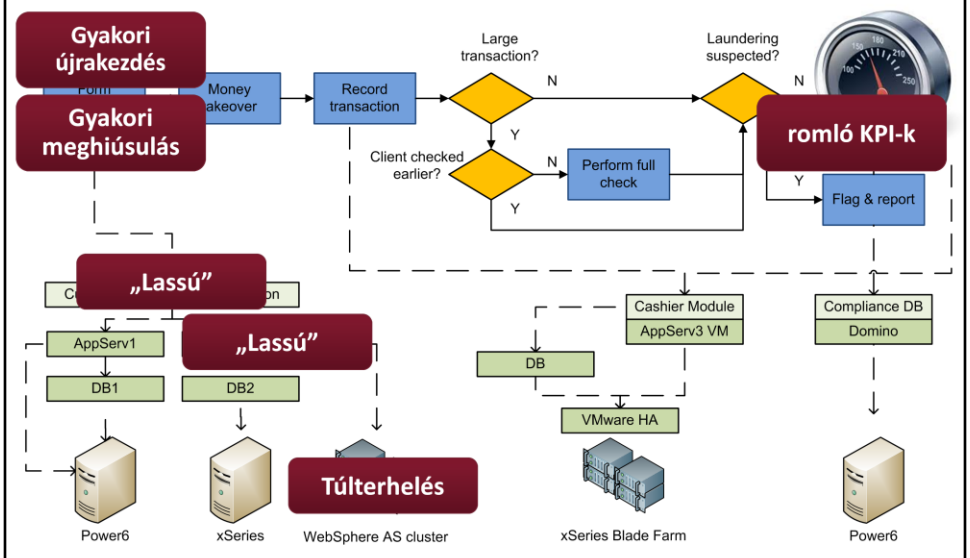
- Milyen részfeladatokból áll?



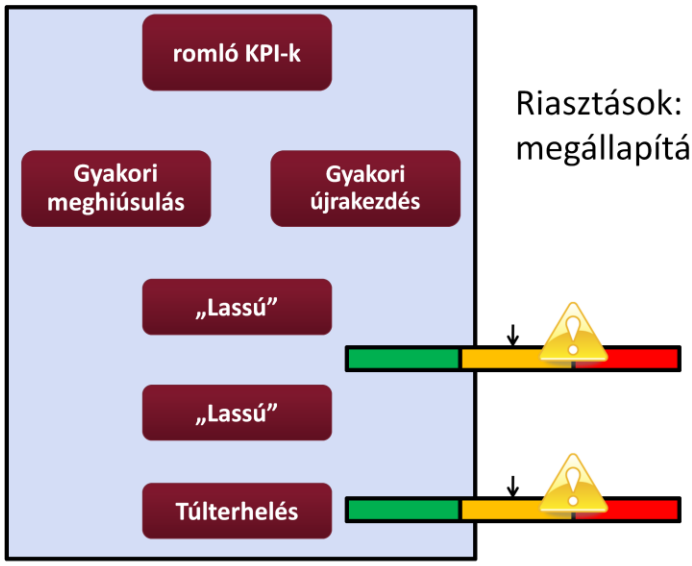
Rendszermonitorozás, mint alapszolgáltatás



Rendszermonitorozás, mint alapszolgáltatás

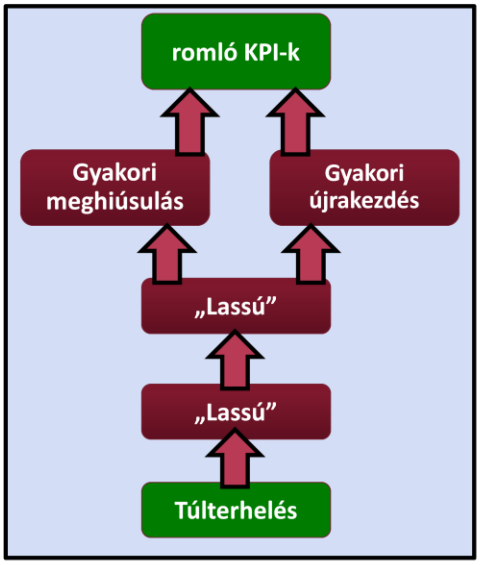


Néhány felügyelet-tervezési feladat



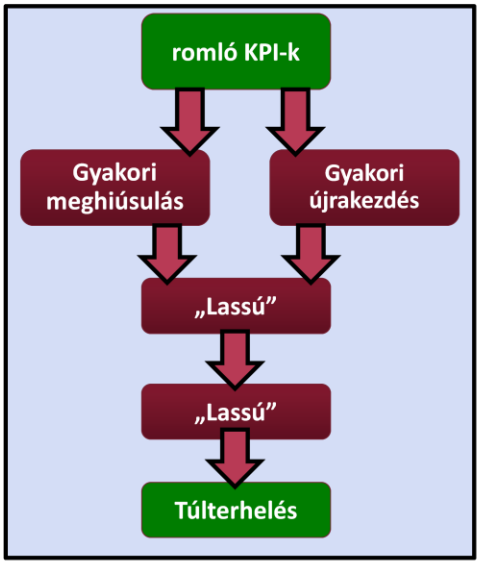
Riasztások: határértékek megállapítása

Néhány felügyelet-tervezési feladat



Eseményfeldolgozás: hatáslánc modellezése

Néhány felügyelet-tervezési feladat

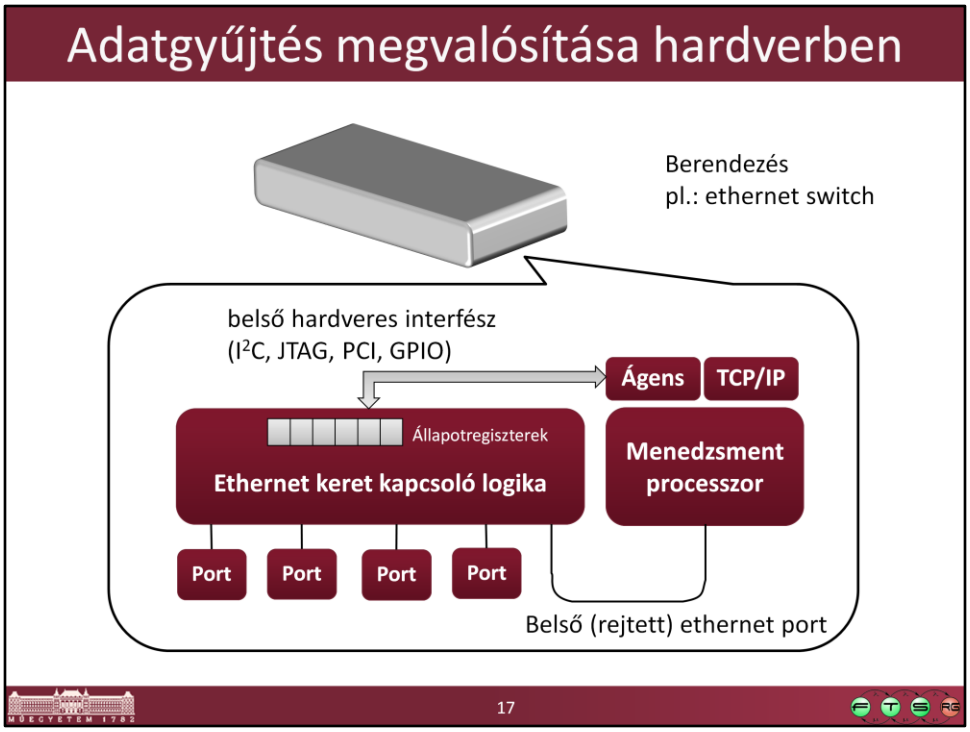


Hibaokok keresése

És így tovább.
Előfeltétel: megfelelő tulajdonságok mérhetősége

Adatgyűjtés megvalósítása

- Jellegzetes követelmény:
  - A rendszerünk nagy, sok különálló elemből áll
  - Az adatokat hálózaton keresztül olvassuk le
- A kulcselem az *ágens*
  - Kis beépülő komponens minden berendezésbe, aminek célja:
    - adatszolgáltatás valamilyen (hálózati) interfészen
    - értesítés különféle események bekövetkezéséről
    - egyszerű beavatkozások elvégzése

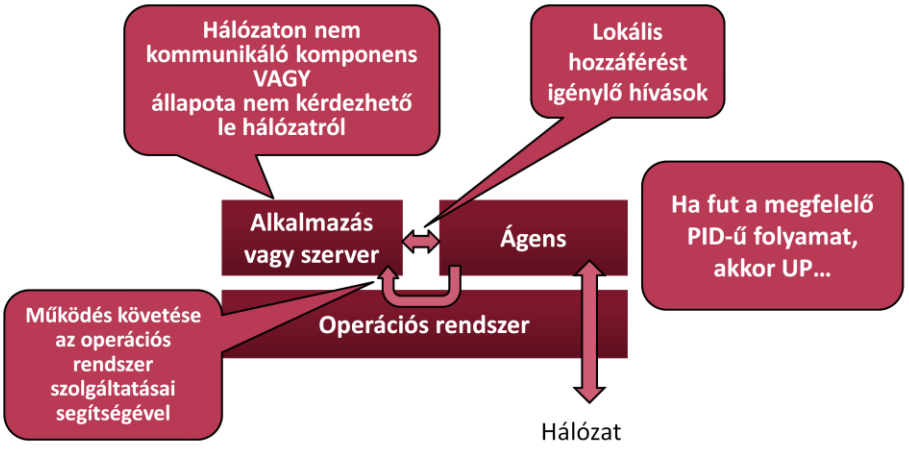


•Az ethernet kapcsoló (switch) csak az ethernet protokoll rétegében működik, nem ismeri a TCP/IP-t
•Hardver állapota belső állapotregiszterekből olvasható ki
•Lehetnek parancsregiszterek is beavatkozásra
•Mindez közvetlen elektromos kapcsolatot igényel, nem vezethető ki a készülékből, vagy legalábbis nagyon kényelmetlen lenne
•Megoldás: helyezzünk el egy kis beágyazott processzort a dobozba, ami közvetlenül össze van kötve a switch hardverrel
•A beágyazott processzoron futó szoftver támogatja TCP/IP protokollkészletet és tartalmazza az ágenst, aminek segítségével a hálózatról lekérdezhetjük a hardver állapotát

Adatgyűjtés megvalósítása szoftverben I.

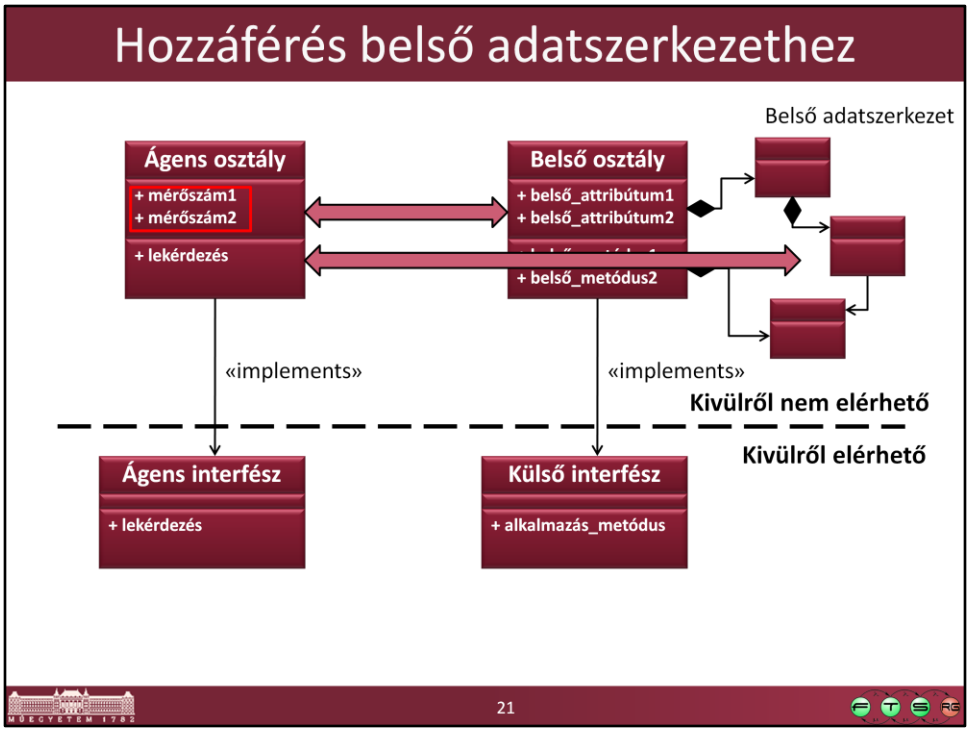
- Jellemző alapesetek:
  - **Olyan szoftver komponenst akarunk megfigyelni, ami nincs erre felkészítve**
    - Az ágens külön folyamat az operációs rendszeren
    - Olyan hívásokat végezhet el, ami csak egy gépen futó folyamatok között lehetséges (de a belső adatszerkezetekhez többnyire nem férünk hozzá)
    - Az operációs rendszer segítségével követi a megfigyelt folyamatot (futási állapot, létrehozott fájlok tartalma, erőforráshasználat, stb.)
  - Az ágens integrált része a szoftvernek

Adatgyűjtés megvalósítása szoftverben I.



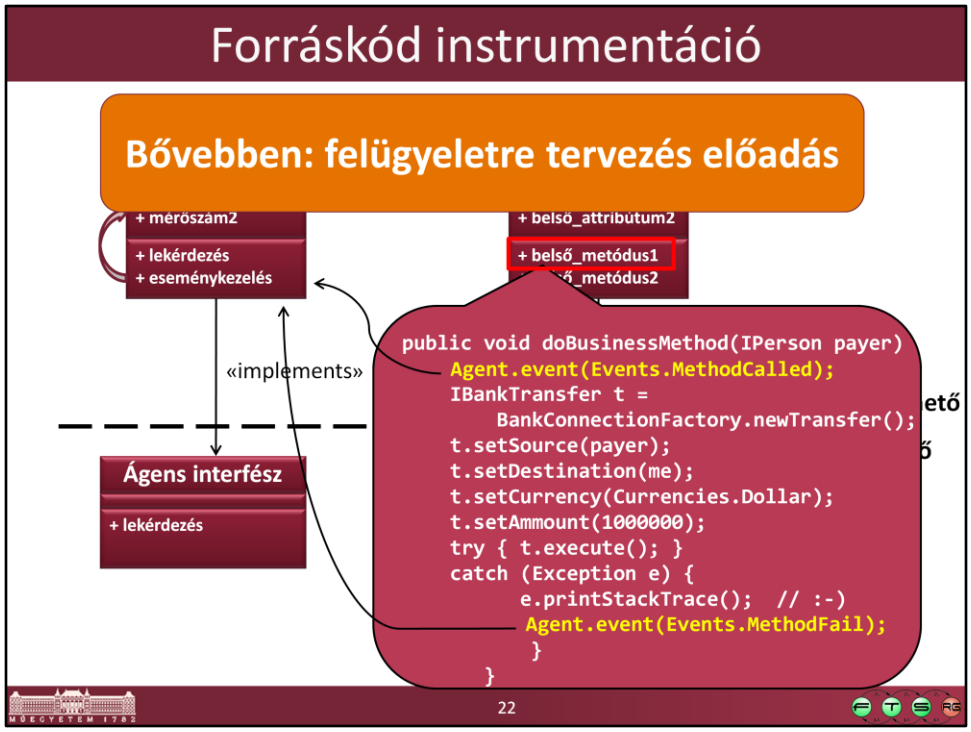
Adatgyűjtés megvalósítása szoftverben II.

- Jellemző alapesetek:
  - Olyan szoftver komponenst akarunk megfigyelni, ami nincs erre felkészítve
  - **Az ágens integrált része a szoftvernek**
    - Hozzáférünk a belső adatszerkezetekhez
    - Közvetlenül végezhetünk függvényhívásokat
    - Forráskód *instrumentálás* (mérő, adatgyűjtő hívások elhelyezése a forráskódban) lehetséges
    - A lényeg: a belső mérési lehetőségeket kívülről is elérhetővé kell tenni



Demonstrációs ábra, ékezet és szóköz valódi modellben ne legyen osztály- és attribútumnévben!

Forráskód instrumentáció



Ágens lekérdezési interfész

- Hogyan kérdezzük le az ágenstől a mért adatokat?
- Jó lenne…
  - hálózaton keresztül
  - szabványos interfész, protokoll
  - Egységesen: gyártók, készülékek, szoftver/hardver
    - Adatok széles skálájának támogatása
  - ha azt is le tudnánk kérdezni, hogy pontosan miket lehet lekérdezni az ágenstől

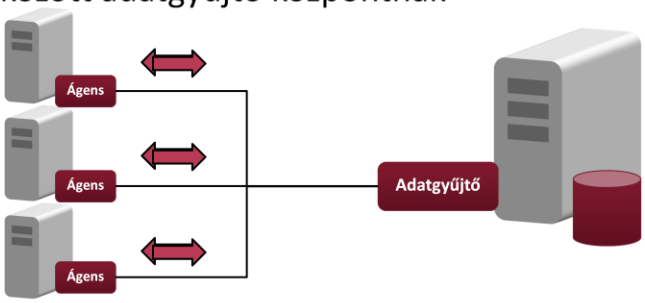
Konfigurációmenedzsment: hasonlóság!

Jellegzetes alapfunkciók

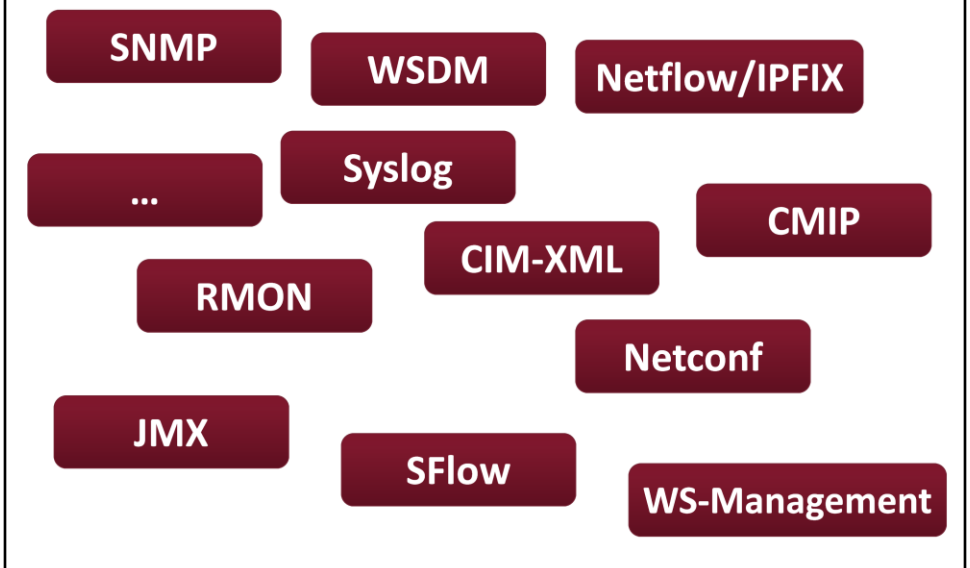
- Pillanatnyi értékek
  - Skalár mennyiség: CPU kihasználtság, RAM, tárhely telitettség, …
  - Diszkrét értékkészlet: Kiszolgáló-folyamat UP/DOWN/ERROR, …
- Összegyűjtött mérési adatok
  - Skalár mennyiség (pl. kumulatív hálózati forgalom)
  - Napló bejegyzések
- Értesítés eseményekről
  - Diszkrét állapotváltozás (ok→down)
  - Határérték túllépés (diszk telitettség >90%)

Ágens lekérdezési interfész

- Ágens interfészek működési elv szerint
  - Pull – a központi adatgyűjtő kezdeményezi az ágensek lekérdezést
  - Push – az ágens kezdeményezi az adatok elküldését a feliratkozott adatgyűjtő központnak

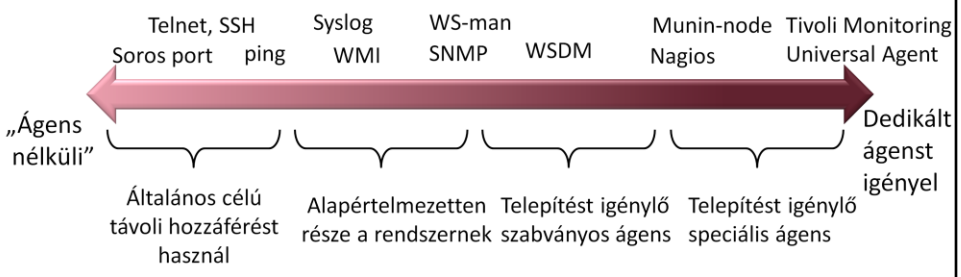


Szabványos protokollok



„Ágens alapú” és „ágens nélküli” technológiák

- Igazából nincs olyan, hogy ágens nélküli
  - Parancssoros belépés és értéklekérdezés: távoli hozzáférés kiszolgáló az „ágens”
  - Inkább: specializáltság alapján

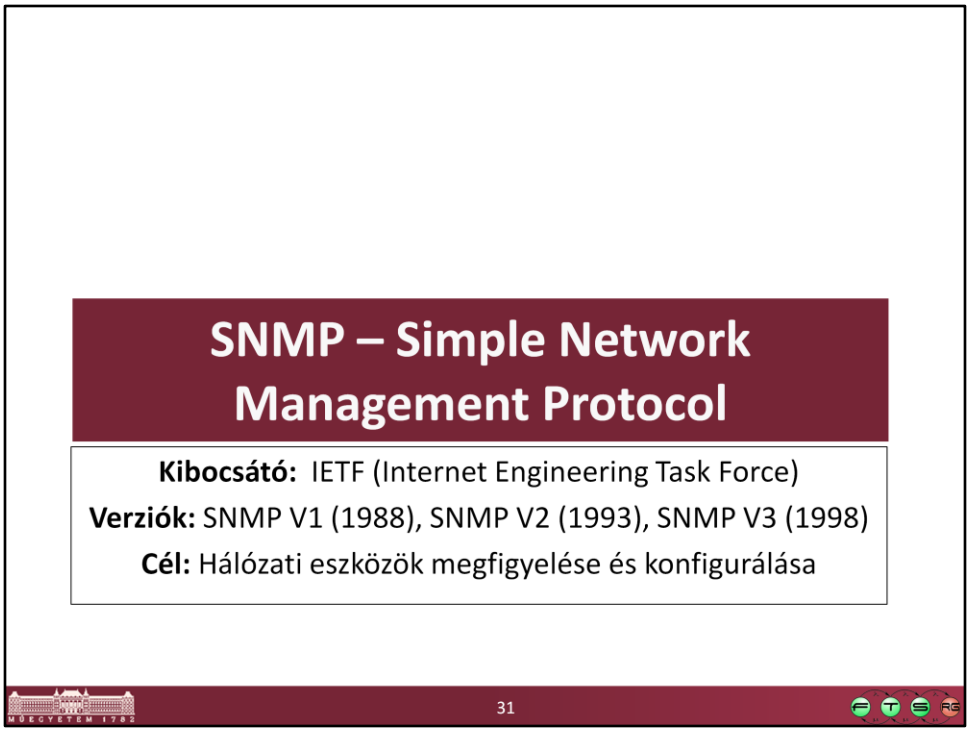


Általános célú távoli hozzáférést használ

Alapértelmezetten része a rendszernek

Telepítést igénylő szabványos ágens

Telepítést igénylő speciális ágens

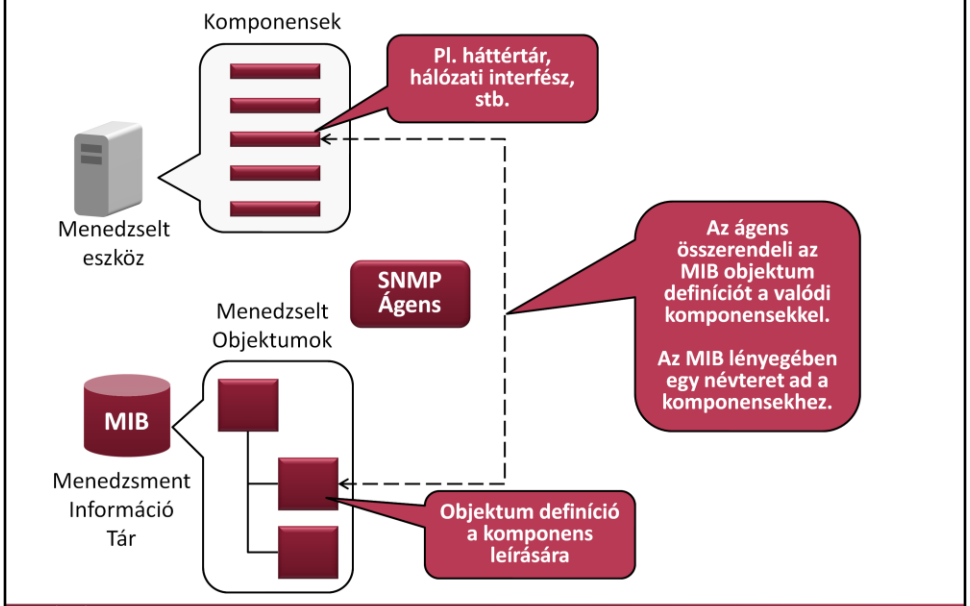


Ha valakinek kimaradt volna az életéből. A lényeg, hogy ezen keresztül látjuk a fő alapelemeket és az egész viszonyát a WBEM témához.

SNMP

- Az SNMP szabvány elemei
  - Lekérdezhető attribútumok szabványos leírása (MIB – Management Information Base)
  - Protokoll az ágens hálózati interfészéhez
    - Értékek lekérdezésre
    - Beavatkozás (attribútum érték beállítása)
  - Eseménykezelés, értesítés (SNMP Trap)
- Nem rögzített
  - Az ágens belső működése
- Nem támogatott
  - MIB struktúra lekérdezése

SNMP


Komponensek
Pl. háttértár, hálózati interfész, stb.
Menedzselt eszköz
SNMP Ágens
Az ágens összerendeli az MIB objektum definíciót a valódi komponensekkel.
Az MIB lényegében egy névteret ad a komponensekhez.
Menedzselt Objektumok
MIB
Menedzsment Információ Tár
Objektum definíció a komponens leírására

SNMP MIB

- MIB szerkezete
  - Fa struktúrába szervezett elemek
  - Minden elemnek egyedi azonosítója (OID)
    - A szintek pontokkal elválasztva
    - Az egyes szinteken belül sorszám
    - OID példa.: `1.3.6.1.2.1.2.1`
      – ember számára értelmezhetetlen
    - Olvasható név (ugyanaz a példa):
      `iso.org.dod.internet.mgmnt.mib-2.interfaces.ifNumber`
      Ez megmondja, hogy hány hálózati interfész van a gépben

OID: ismerős kell, hogy legyen az LDAP világából

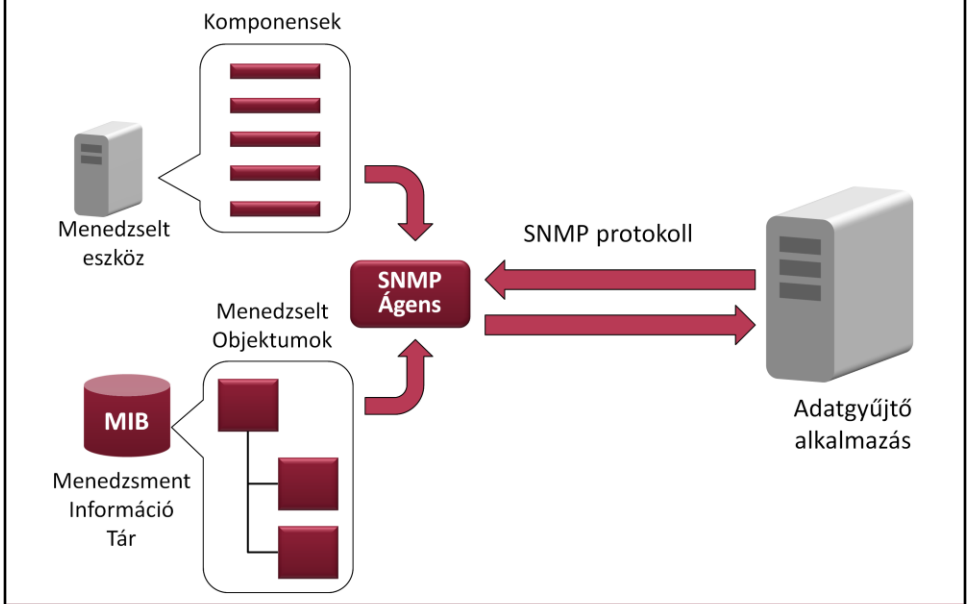
SNMP MIB „metamodellje”

- MIB elemfajtái
  - ObjectIdentifier (szervezőelem, ~csomag)
  - ObjectType (objektum definíció ~osztály)
    - Alaptípusok:
      - Integer
      - DisplayString
      - Gauge
      - INTEGER felsorolt értékkészlettel (~enumeráció)
    - Sequence – objektum több attribútummal
    - SequenceOf (más néven Table) – tömb egy Sequence típusból
  - Elemek között csak tartalmazási kapcsolatot ismer

SNMP MIB

- Az MIB kiterjesztése
  - MIB „metamodell” – TXT file-okban terjesztett ASN definíciók
  - Gyártóspecifikus kiegészítések az `iso.org.dod.internet.private` (`1.3.6.1.4.`) alá
  - Az ágens által támogatott kiegészítést külön kézzel hozzá kell adni a menedzselő alkalmazáshoz
  - Nem kérdezhető le, hogy az ágens milyen MIB kiegészítéseket ismer

SNMP


Komponensek
Menedzselt eszköz
SNMP protokoll
SNMP Ágens
Menedzselt Objektumok
MIB
Menedzsment Információ Tár
Adatgyűjtő alkalmazás

SNMP

- MIB viszonya a CIM-hez
  - Hasonló szerepet lát el: objektum definíciós séma
  - ASN.1 is leképezhető osztálystruktúrává (~MOF megfelelője)
- SNMP MIB-ből hiányzik
  - Referencia más objektumra, csak string alapú nevekkel és azonosítók egyezőségével lehet ilyet kifejezni
  - Öröklődés az osztályok között
  - Meta lekérdezési lehetőségek
  - Dinamikus osztály példány kapcsolat – az MIB statikus szerkezetet ír le, csak a Table soraival fejezhető ki dinamikus struktúra
  - Ebből következően az MIB nem igazán konfiguráció menedzsment adatbázis

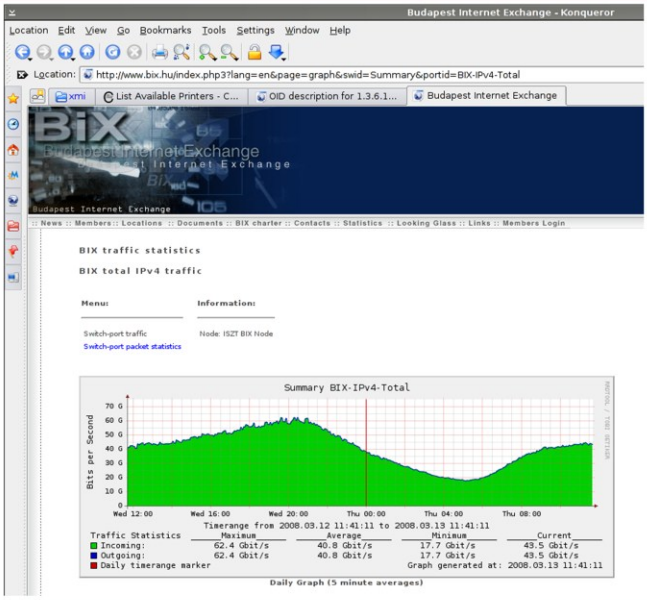
SNMP

- SNMP viszonya a WBEM-hez
  - Mindkettő távoli lekérdezésre és módosításra szolgál
  - Mindkettő nyílt szabvány
- Eltérések
  - Az SNMP saját bináris protokollt használ, nem XML-t
  - Az SNMP kliensnek kell tudnia, hogy mit támogat az ágens – kézi konfigurálást igényel, nem kellően automatikus
  - Az SNMP-t gyakorlatilag nem használják beavatkozásra, konfigurálásra (pedig lehetne)

SNMP

- Gyakorlati alkalmazási példa:
  MRTG (Multi Router Traffic Grapher)
  - Hálózati forgalom monitorozás
  - Periodikus lekérdezés
  - Historikus adat tárolás (rrdtool, round-robin database)
  - Grafikon generálása
  - Webes felületen elérhető
  - Használja például: BIX (Budapest Internet Exchange)

MRTG alkalmazási példa: BIX

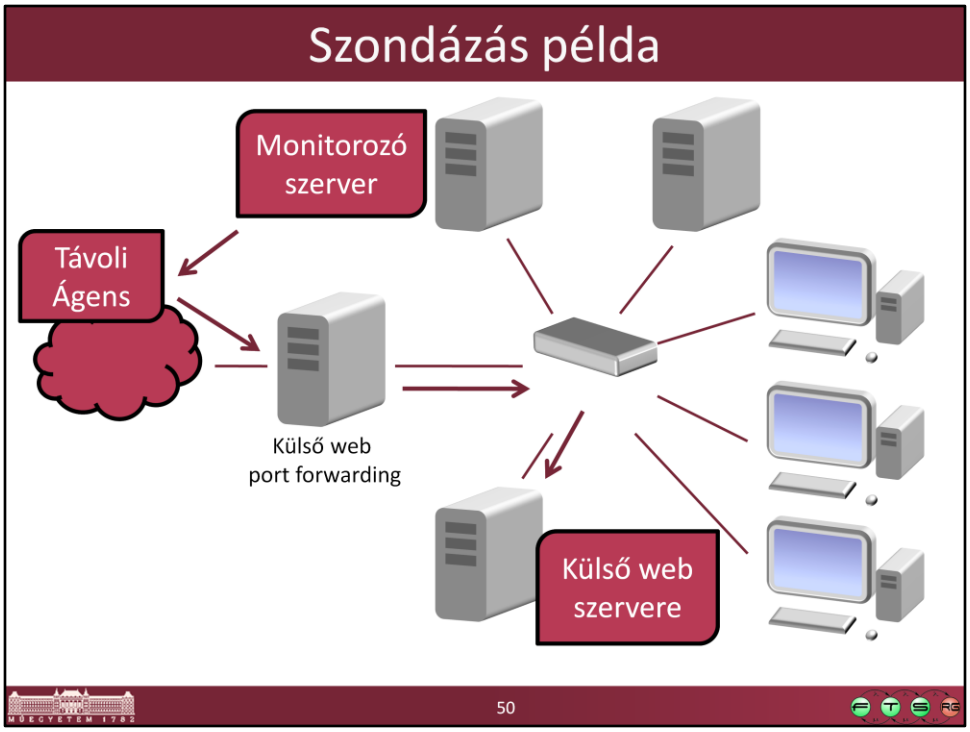


DEMO Windows 7 SNMP MIB bejárása

- SNMP szolgáltatás: „Turn Windows features on or off”
  - Majd Services-ben tulajdonság-beállítások; legalább olvasó SNMP community
- MIB tallózása
  - OidView Professional (7 napos próbaváltozat)
  - Néhány F/OSS opció: SnmpB, MBJ

Szondázás

- Szondázás - probing
  - Tipikusan „ágens nélküli” megközelítés: ha nem belenézni akarunk a célrendszerbe, hanem a távolról elérhető szolgáltatását kipróbálni
  - Ilyenkor a monitorozó rendszer, mint hálózati kliens próbál igénybe venni egy szolgáltatást
  - Ilyenkor is szükség lehet ágensre
    - Meghatározott **szolgáltatás elérési pontról** (Service Access Point) nézve akarunk képet kapni a szolgáltatásról



A külső webnek, mint szolgáltatásnak a megcélzott szolgáltatás elérési pontja a tűzfalon kívül van -> akkor van „jó” állapotban a külső web, ha kívülről nézve működik. A monitorozó szerver viszont belül van, ezért kell egy távoli ágens, amit megkérhet, hogy kívülről is megnézze a szolgáltatást.

Táblánál Szondázás

- End-to-end-probing: infrastrukturális elemek állapotának hatása a szonda kimenetére
- Egyszerűsített mátrix alapú modellezés
- A minimális hibadetektáló szondahalmaz problémája
- A minimális hibadiagnosztizáló szondahalmaz problémája

DEMO Központi adatgyűjtő és megjelenítő

- Nagios
  - Free, open source
  - http://www.nagios.org/
  - Kevés (<100) gép megfigyelése esetén jó megoldás
  - Elsődlegesen a pillanatnyi állapot áttekintésére és automatikus riasztásra való
- Tactical overview
  - Monitorozott szolgáltatások
  - Grafikus megjelenítés
- Rendelkezésre állás és teljesítmény jelentés
- Naplók és riasztások
- Főleg aktív szondázásra alapoz, kézi konfigurálást igényel
- Saját ágens protokollja is van,
  - Egyszerű szöveges protokoll, könnyen bővíthető shell scriptekkel
  - Támogat szabványos protokollokat is

Historikus adatgyűjtés

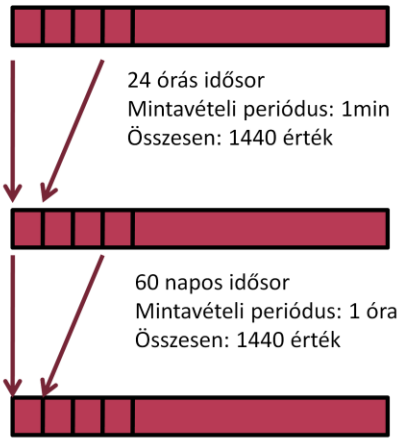
- De jó lenne, ha…
  - Visszamenőleg látnánk, hogy mi történt
  - Látnánk a tendenciákat
  - Következtetéseket vonhatnánk le. Pl.:
    - Mi van túlterhelve, mi nincs kihasználva (bővítés tervezése)
    - Hogy néz ki, amikor 500 hallgató megrohanja a szervert ☺
    - Mennyi idő alatt sülnek meg a gépek, ha leáll a klímaberendezés (katasztrófa elhárítási terv)
    - Nem kezdett-e el valami elfogyni/elhasználódni, amit majd cserélni, pótolni kéne? (Proaktív beavatkozás) Pl. szabad tárhely, UPS akkumulátorok, merevlemezek, nyomtató toner stb.

Historikus adatgyűjtés

- Megoldás
  - Periodikusan (mondjuk percenként mintavételezve) tároljuk el a mért értékeket
  - Mi ezzel a baj?
  - Számoljunk utána: belefulladunk az adathalmazba
  - Biztos, hogy tudni akarjuk, hogy pontosan mi történt 1 éve 5 hónapja, 13 napja, 8 óra 13 perce?
  - Attól függ:
    - Trend megállapításhoz: ilyen pontosan nem, de azért hozzávetőlegesen igen
    - Konkrét esemény dokumentálásához: kell a nagy pontosság

Historikus adatgyűjtés

- Aggregáció
  - „Adattárházas” fogalom
  - Több adatot vonunk össze egyetlen értékbe (felbontás rontás, pl átlagolással)
  - Mit veszítünk vele?
    - Konkrét, rövid események lefutása
    - Börsztösség
  - Mit lehet tenni ellene?
    - külön archiválni kell az „érdekes” részeket -> eseménykorreláció
    - Összevont MIN/MAX/AVG értéket tárolni



DEMO Historikus adatgyűjtés

- Munin
  - Free, open source
  - http://munin.projects.linpro.no/
  - Kevés (<20-50) gép megfigyelése esetén jó megoldás
  - Elsődlegesen tendenciák rögzítésére grafikonon ábrázolásra
  - Összekombinálható Nagios-szal riasztásra
- RRDtool-ra épül (hasonlóan az MRTG-hez)
  - Ez biztosítja az időbeli aggregációt (round-robin database)
  - RRDGraph generál grafikonokat, webes felületre
- Saját ágens protokollja van (rendkívül egyszerű szöveges)
  - Plugin architektúra, könnyen bővíthető saját shell scriptekkel
  - Automatikus szerver-oldali konfiguráció: az ágens bejelenti, hogy milyen értékeket mér