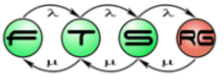
Intelligens rendszerfelügyelet (VIMIA370)

Eseménykezelés

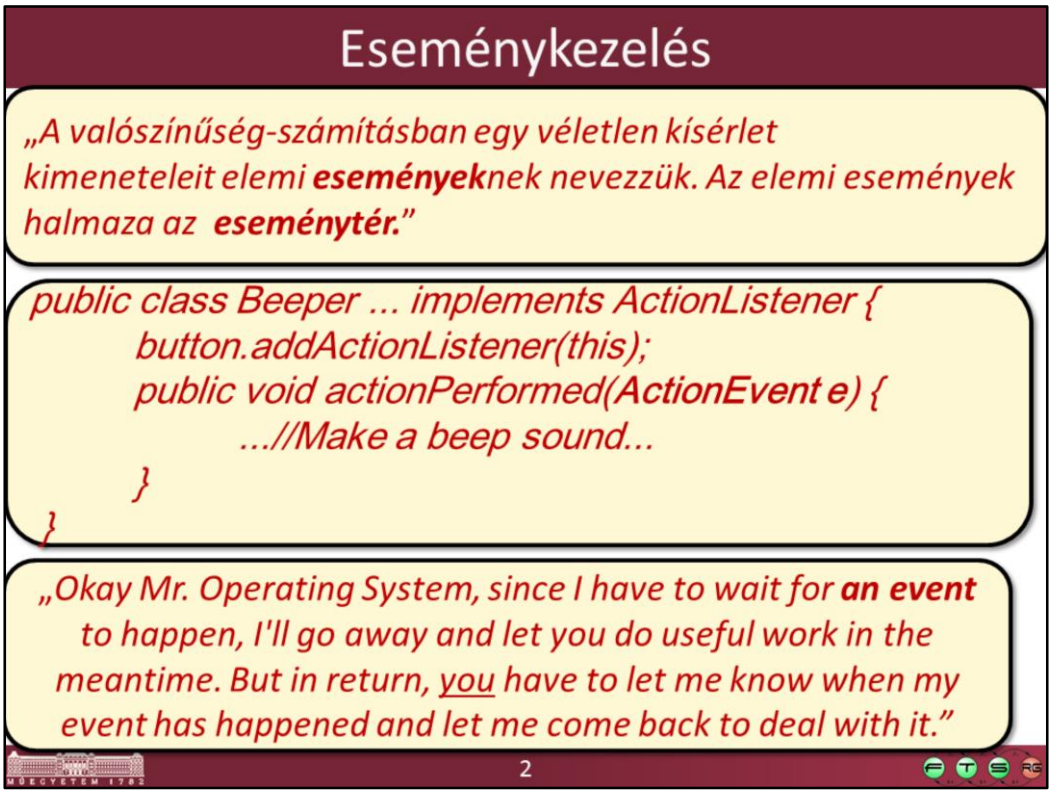
Kocsis Imre, Micskei Zoltán, Salánki Ágnes



Budapesti Műszaki és Gazdaságtudományi Egyetem
Méréstechnika és Információs Rendszerek Tanszék

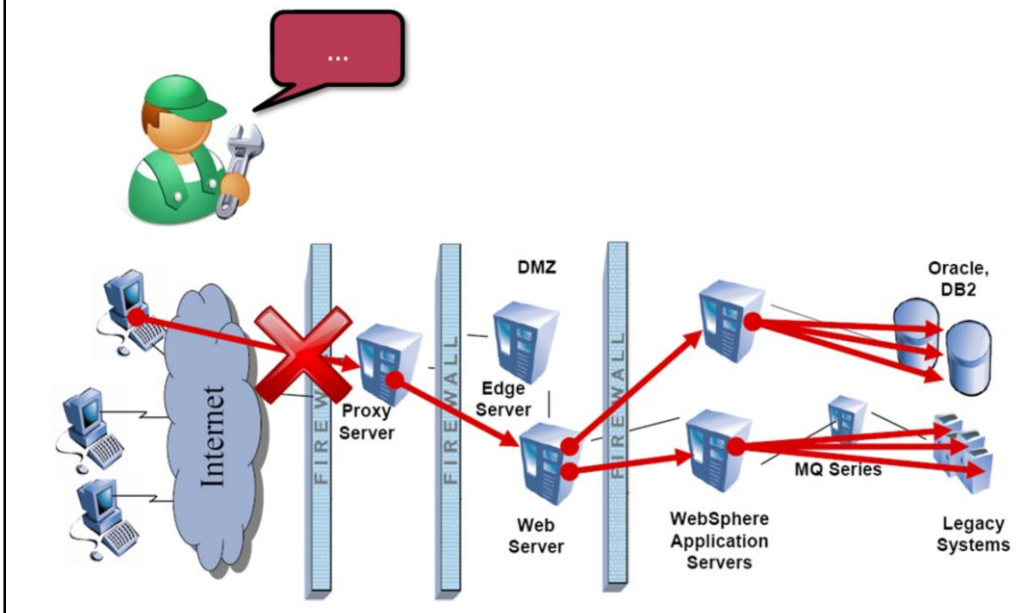
Utolsó módosítás: 2016. 04. 25.

Gönczy László és Dávid István fóliáit felhasználva (Komplex eseményfeldolgozás rész)

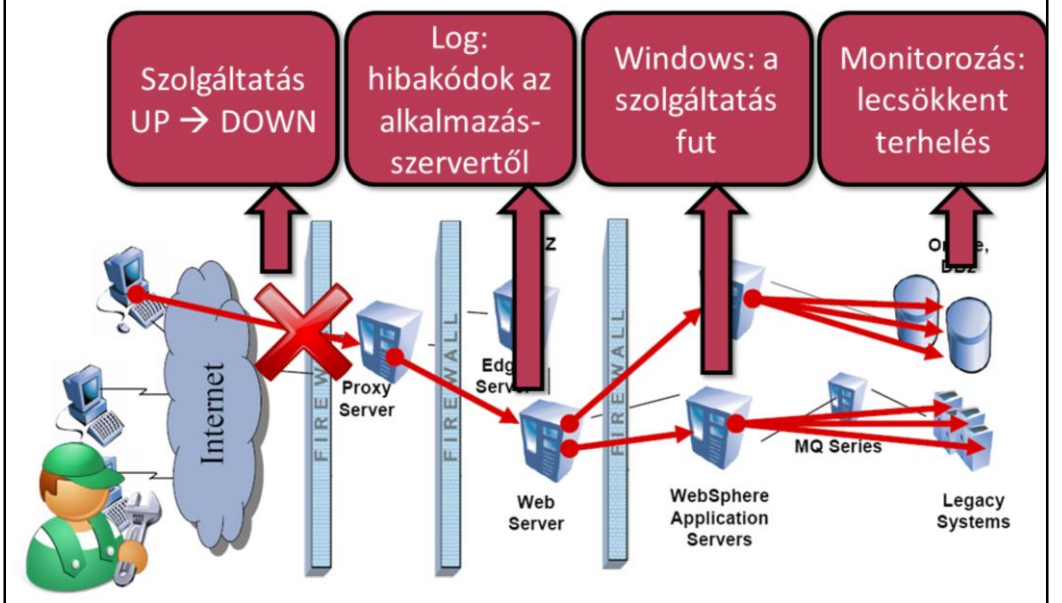


Korábban is már sok tantárgyban, többféle értelemben találkoztunk az esemény fogalmával.

Motiváció


...
Internet
FIREWALL
Proxy Server
FIREWALL
DMZ
Edge Server
Web Server
FIREWALL
Oracle, DB2
MQ Series
WebSphere Application Servers
Legacy Systems

Motiváció

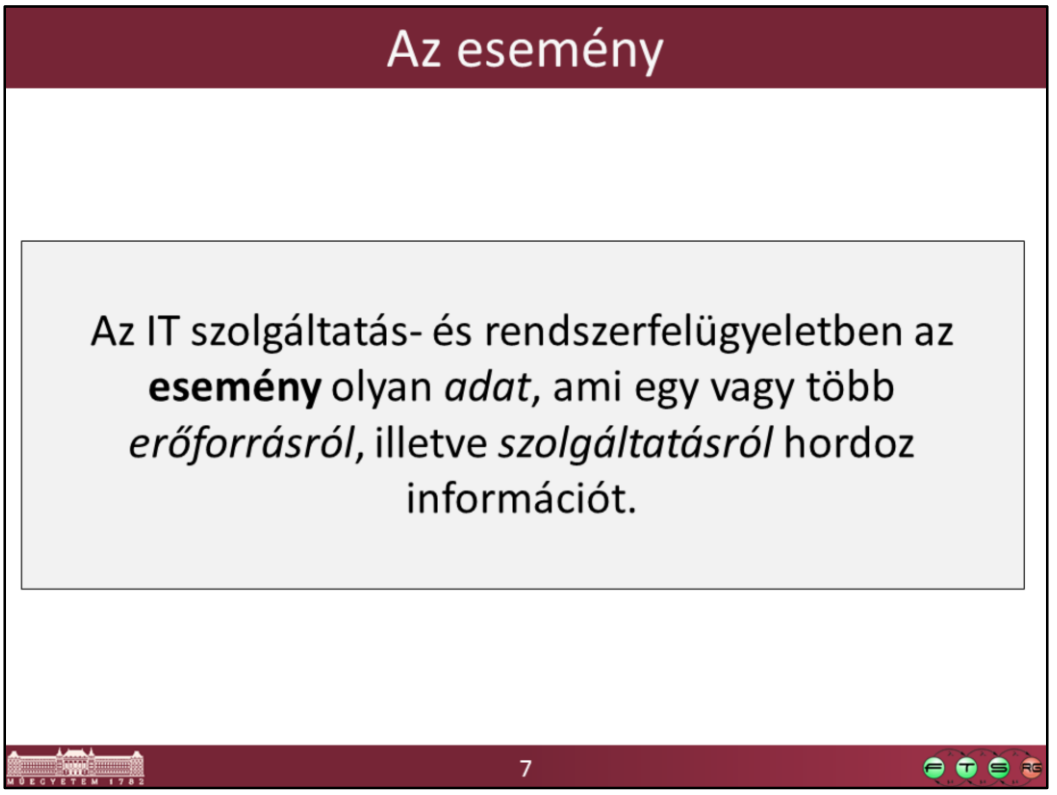

Szolgáltatás UP → DOWN
Log: hibakódok az alkalmazás-szervertől
Windows: a szolgáltatás fut
Monitorozás: lecsökkent terhelés
Internet
FIREWALL
Proxy Server
Web Server
WebSphere Application Servers
MQ Series
Legacy Systems

Motiváció

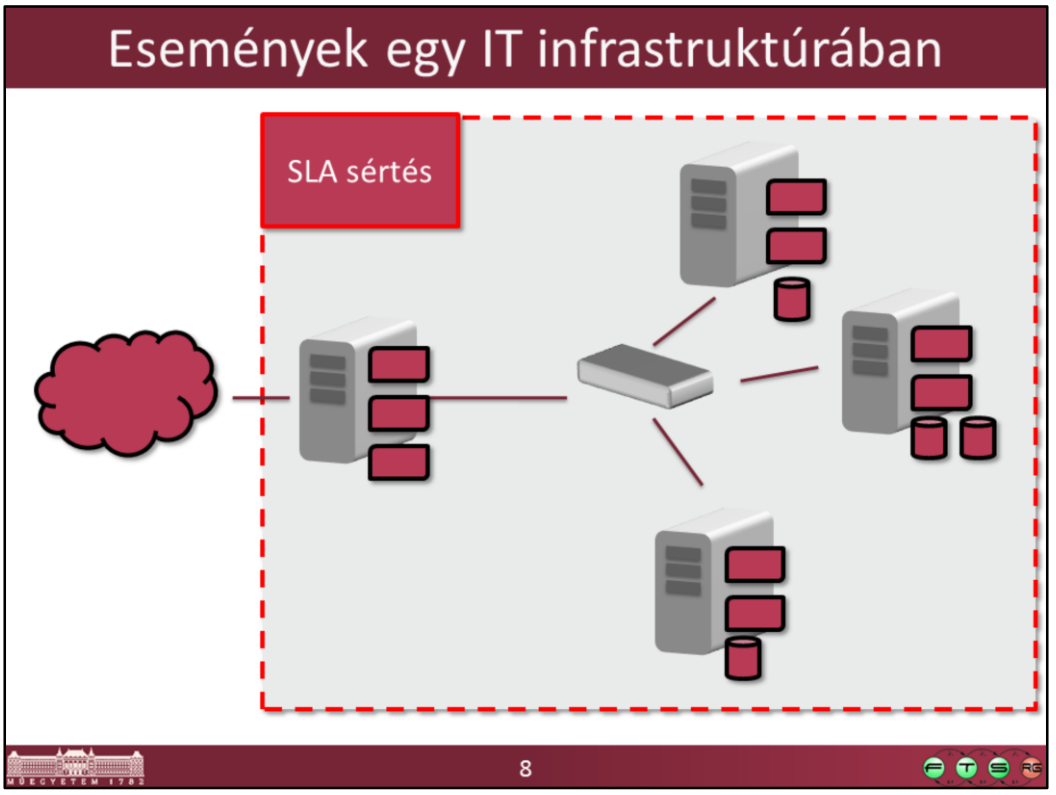

Az események széleskörű figyelése elengedhetetlen; igaz, sok egyidejű esemény intelligens feldolgozása nehéz.
Internet
FIREWALL
Proxy Server
FIREWALL
DMZ
Edge Server
Web
FIREWALL
Oracle, DB2
MQ Series
Legacy Systems
Naplózás ≠ eseménykezelés!

Tartalom

- IT esemény fogalma
- Eseménykezelés folyamata
- Megvalósítások (Eventlog, syslogd)
- Kitekintés: komplex események feldolgozása

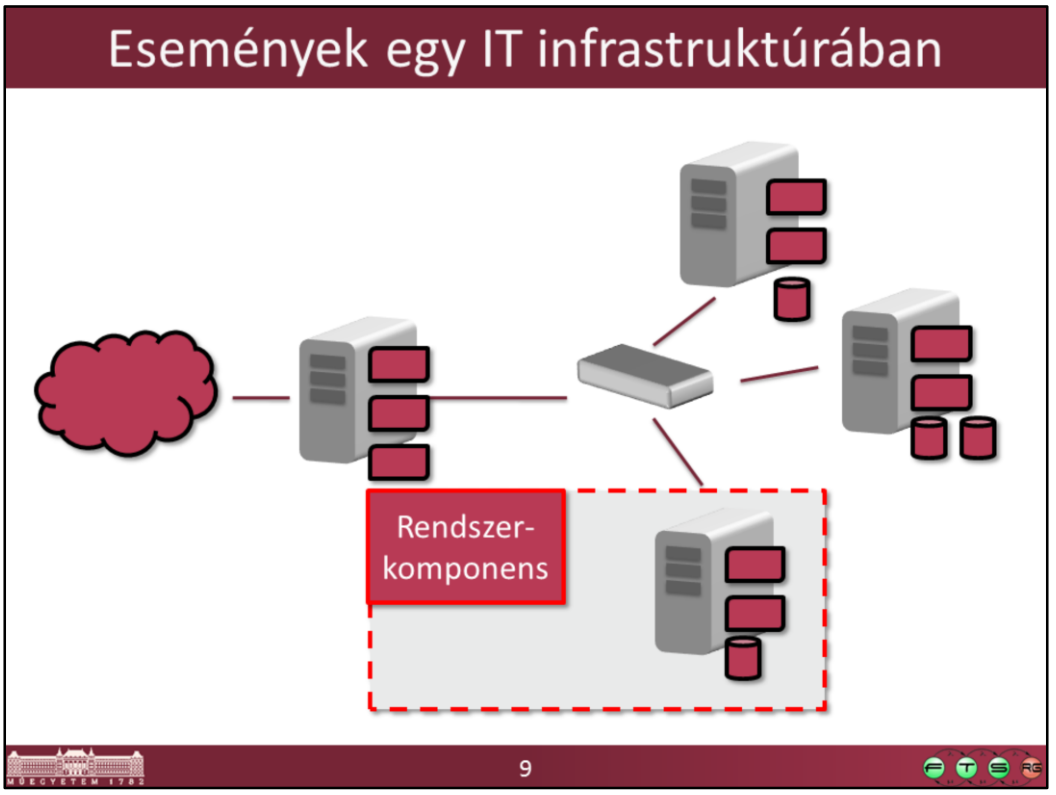


További szűkítések nélkül sajnos tényleg csak ennyire általános definíció adható.



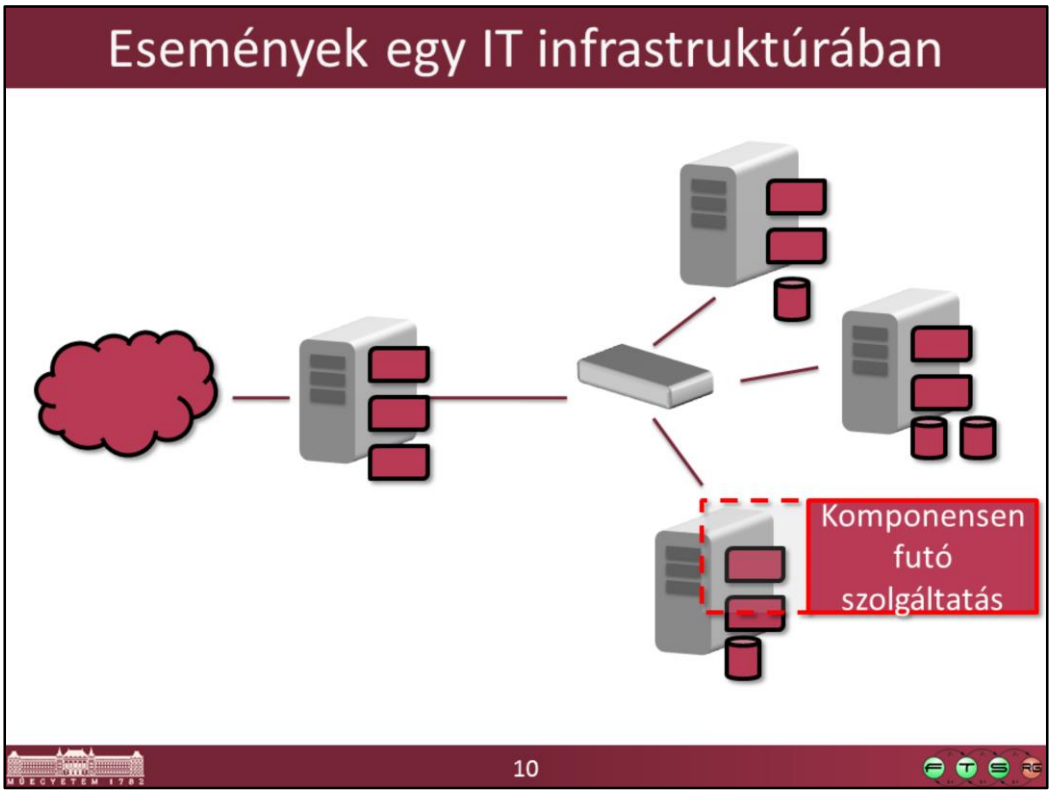
Service Level Agreement-ek eseményei

- SLA megsértése (SLA breach)
- SLA-sértés közeli állapotba kerülés
- …

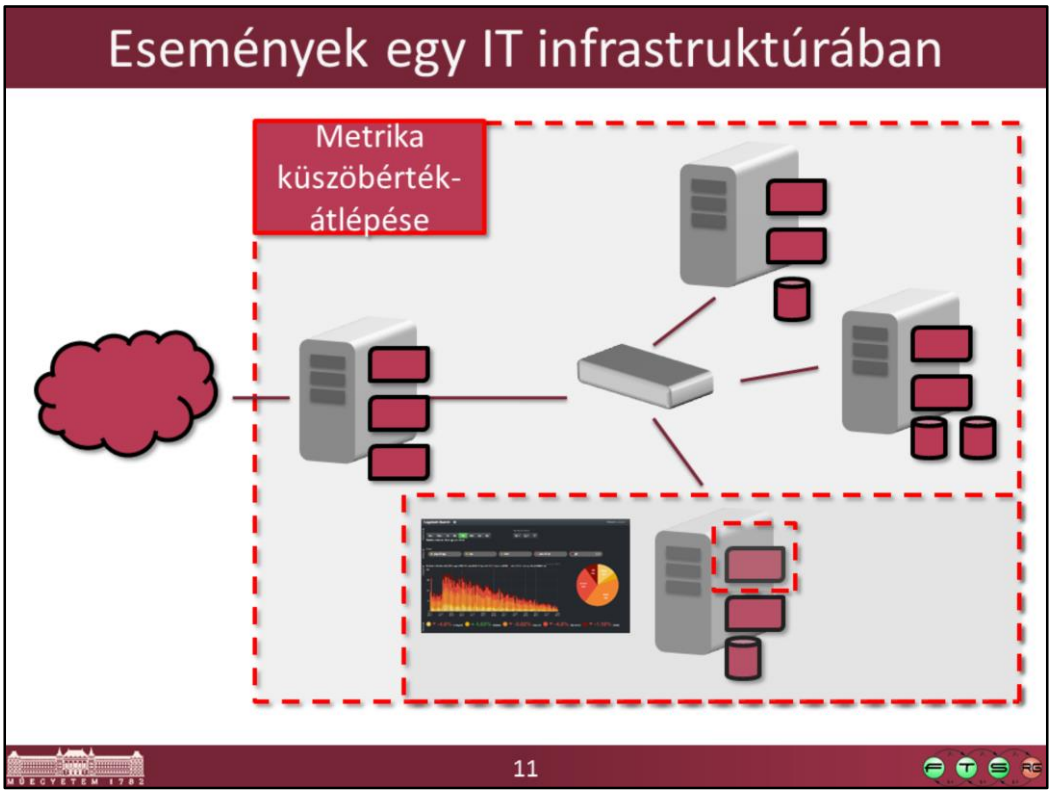


Rendszerkomponensek működési mód- és állapotváltásai

- Warning: DB2 has started ☺
- Konfiguráció megváltozása
- …

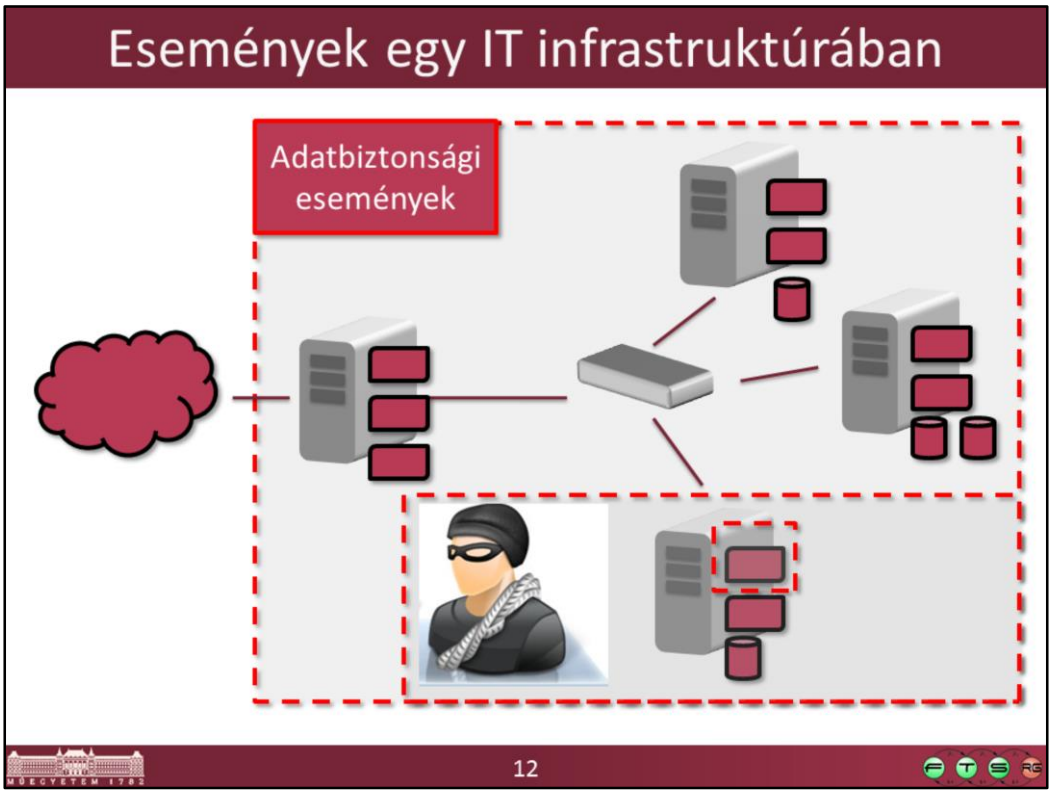


Apache access log
Új felhasználó került felvételre
…



Egy komponensen értelmezett metrikák megváltozása, vagy küszöbérték-átlépése

- Web szerver lecsökkent válaszideje
- Túl magas processzorhasználat
- Szolgáltatás túl alacsony rendelkezésre állása
- …

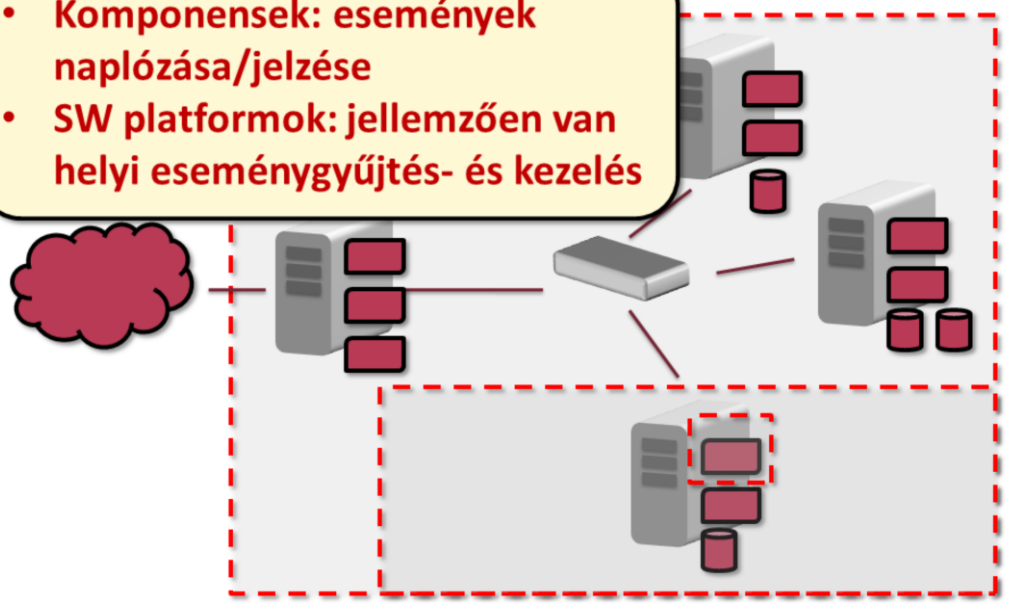


Adatbiztonsági események

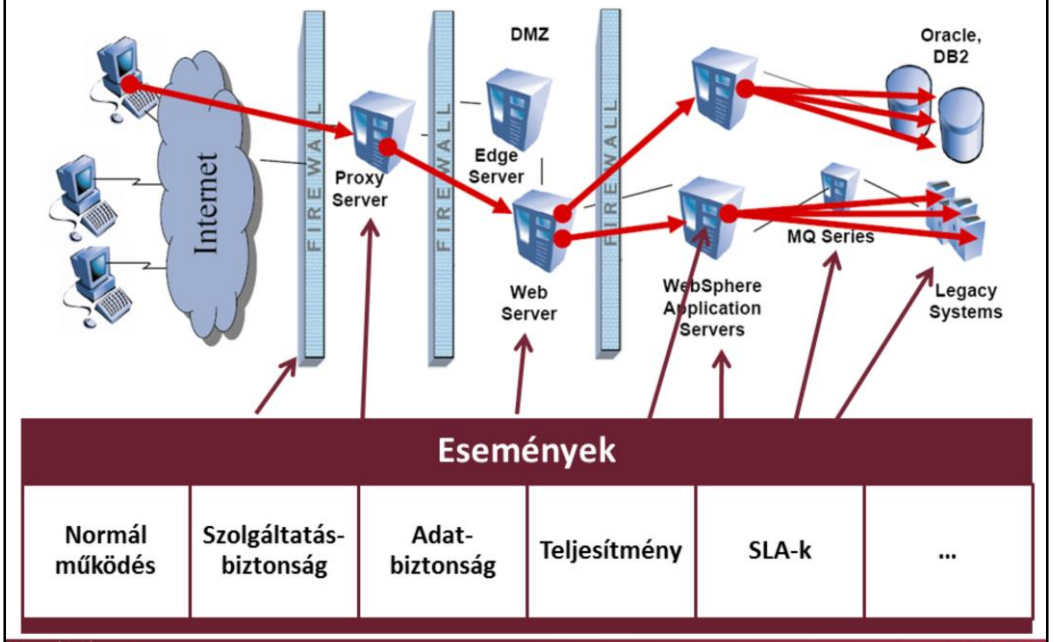
- Sebezhetőség megjelenése
- Támadási kísérlet
- Bizalmasság, integritás vagy rendelkezésre állás sérülése

Események egy IT infrastruktúrában

- **Komponensek: események naplózása/jelzése**
- **SW platformok: jellemzően van helyi eseménygyűjtés- és kezelés**

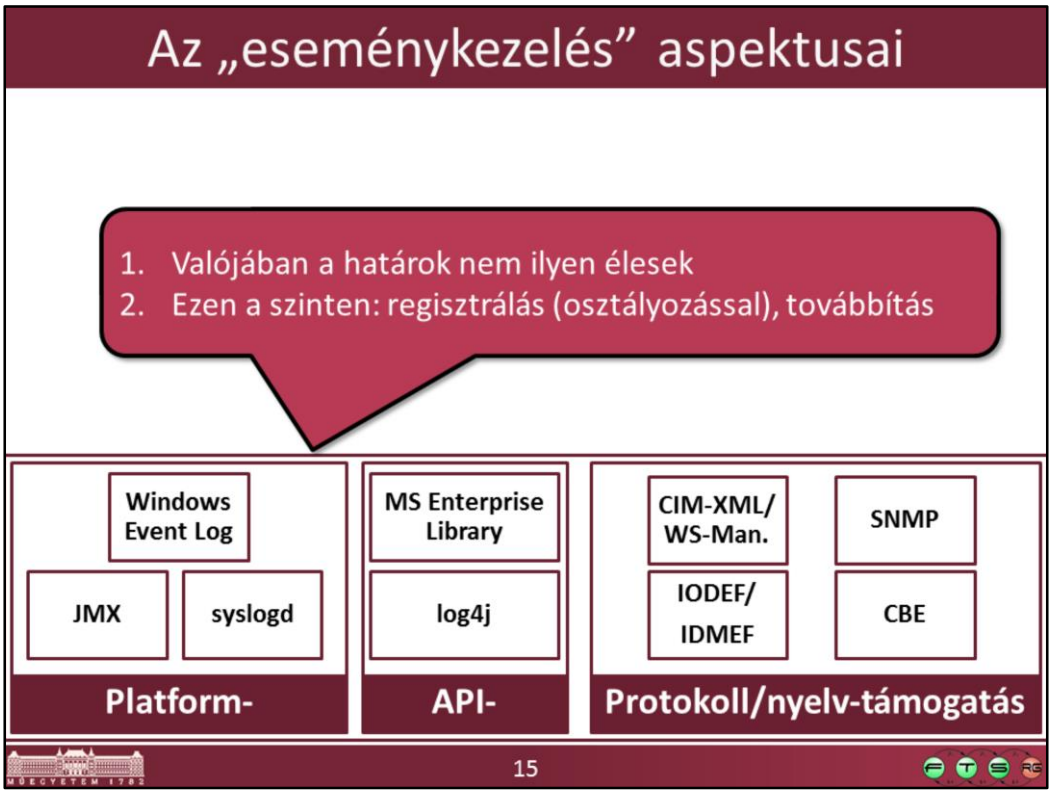


Események egy IT infrastruktúrában

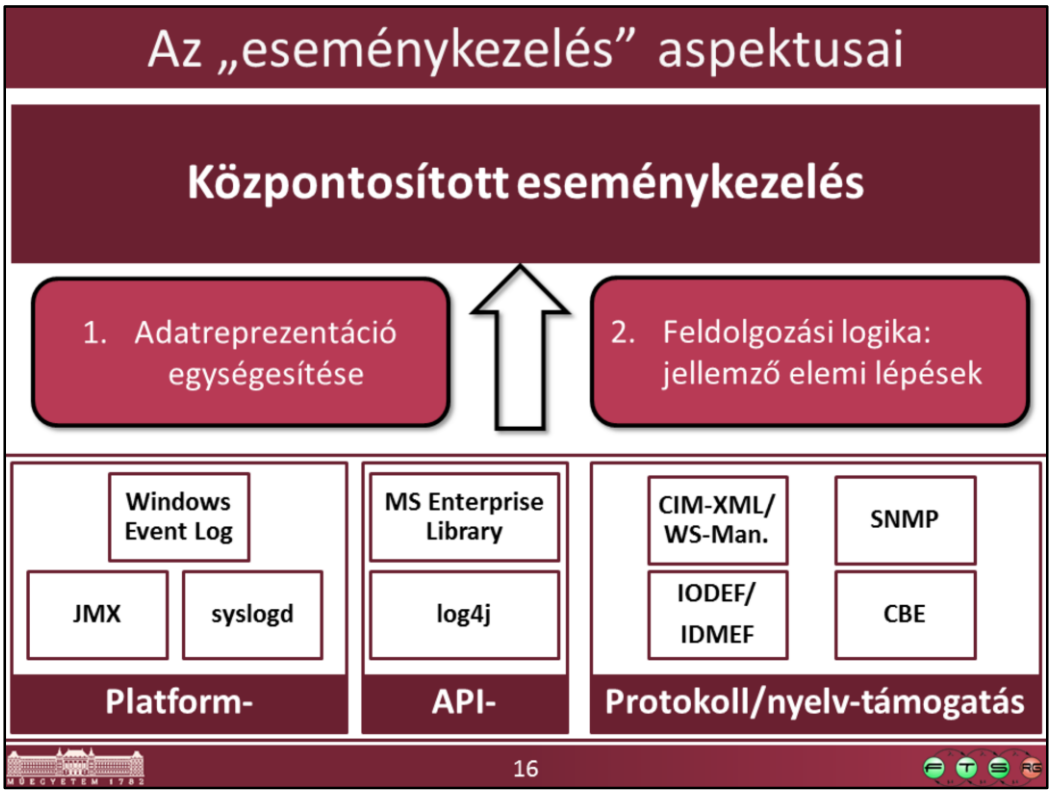


Események

Normál működés	Szolgáltatás-biztonság	Adat-biztonság	Teljesítmény	SLA-k	...



A Microsoft Enterprise Library („a set of tools and programming libraries for the Microsoft .NET Framework”) „Logging Application Block”-ja ad loggolást támogató API-t és mechanizmusokat; ez sokban hasonlít pl. a log4j-re a Java világból (Rendszerfelügyeletre tervezés labor).
A már megismert protokollok mind támogatják események átvitelét (a saját adatmodelljük kontextusában értelmezve azokat); említést érdemelhet még pl. a „Common Base Event” (http://www.ibm.com/developerworks/library/specification/ws-cbe/) leírónyelv és az Incident Object Description and Exchange Format (IODEF - http://xml.coverpages.org/iodef.html) / Intrusion Detection Message Exchange Format (IDMEF - http://www.ietf.org/rfc/rfc4765.txt).
Figyelem: a listák legjobb esetben is csak reprezentatívak, nem pedig teljesek.



Az adatreprezentáció egységesítésével nem foglalkozunk (arra lásd például a CBE-t); amit tárgyalunk: mik azok az eleminek tekinthető feldolgozási lépések/minták, amikből az eseményfeldolgozás logikáját fel szokás építeni.

ESEMÉNYKEZELÉS FOLYAMATA

ITIL definíciók az egységes eseménykezeléshez

Esemény-feldolgozás

- Események gyűjtése és (fél)automatikus feldolgozása rendszerfelügyeleti szoftverekkel
- Eseményforrások és eseményfeldolgozók
  - Feldolgozók: eseményfeldolgozási hierarchia

Egységes adatreprezentáció: eseményfolyam + állapotok

- Naplózás: az események megváltoztathatatlanok
- Eseményfeldolgozás:
  - „alert” szemantika (→ megszűnhet)
  - módosítható állapot/tulajdonságok
    - lezárás, szelektív törlés, „elnyomás”…
- Lehetséges bemenet
  - **Eseményfolyamként**
  - Eseményfelhőként

Az adatfolyamok kezelése sokkal nehezebb, mint úgy általában a batch-ben kapott adatok feldolgozása, a kezdetekkor például ott van az időzítés problémája (fizikai, logikai óra stb., majd MSc-n tanulható).

Megváltoztathatatlan = immutable

Egységes adatreprezentáció: esemény, mint megfigyelés

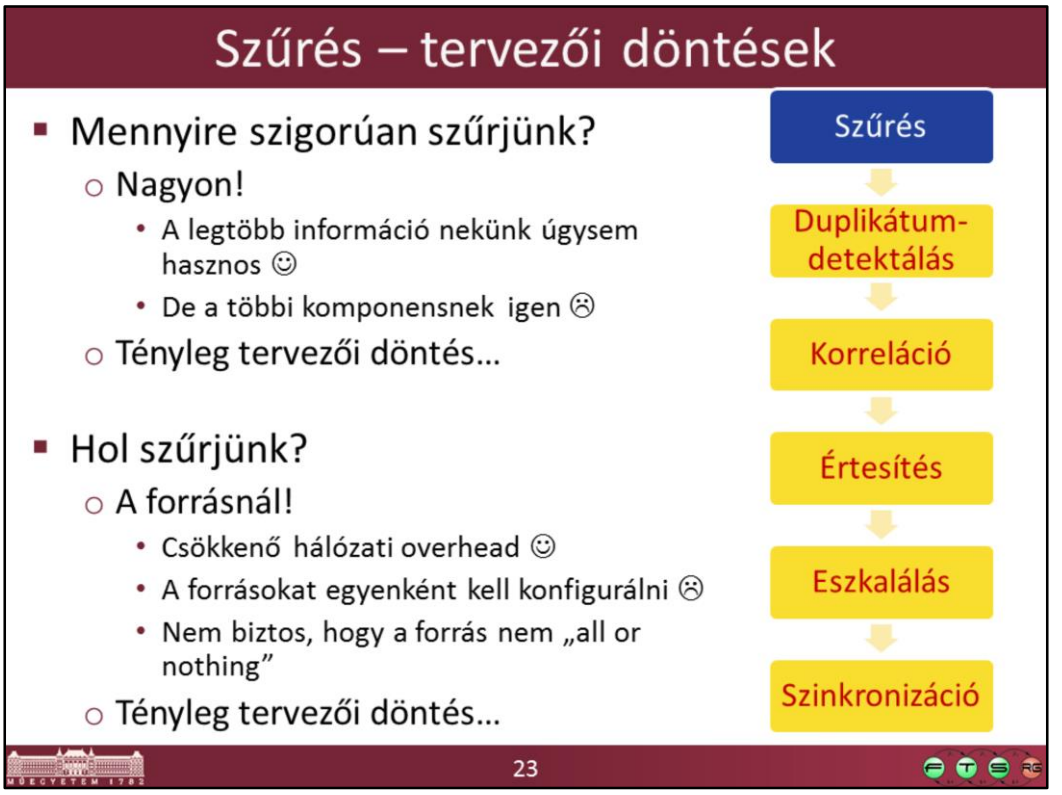
- Időbélyeg
- Forrás (komponens, felhasználó, folyamat stb.)
- Üzenet tartalma
- Súlyosság
  - Beépített/alapértelmezett
  - „Business impact” alapján
    - Fatal – sok felhasználót érint, azonnal reakció igényelt: „paging”
    - Warning – kevés felhasználót érint, „ez még várhat”
    - …

Warning: DB2 has started ☺

A feldolgozás jellemző lépései

Szűrés

- *Az a folyamat, melynek célja egy szabályrendszer alapján történő „információblokkolás”.*
- Feldolgozandó/továbbítandó adatmennyiség csökkentése
  - Pl. feldolgozási és hálózati kapacitás korlátok miatt
- Redundáns információ eltávolítása
  - Pl. több ágens ugyanazt az objektumot figyeli



Hogyan szűrünk?

1. Mindent, ami nem fatal vagy warning, azt dobjuk el, úgysem jelent semmit → más komponenseknek ettől még ez az információ hasznos lehet
2. Jóval engedékenyebbek vagyunk, cserébe nő az adatmennyiség

Hol szűrjünk?

1. Minél közelebb a forráshoz, hogy elkerüljük a számítási és hálózati többletköltséget
2. A forrásnál nem tudunk szűrni, mert „the event generator itself is an all-or-nothing implementation”.

Duplikátumdetektálás

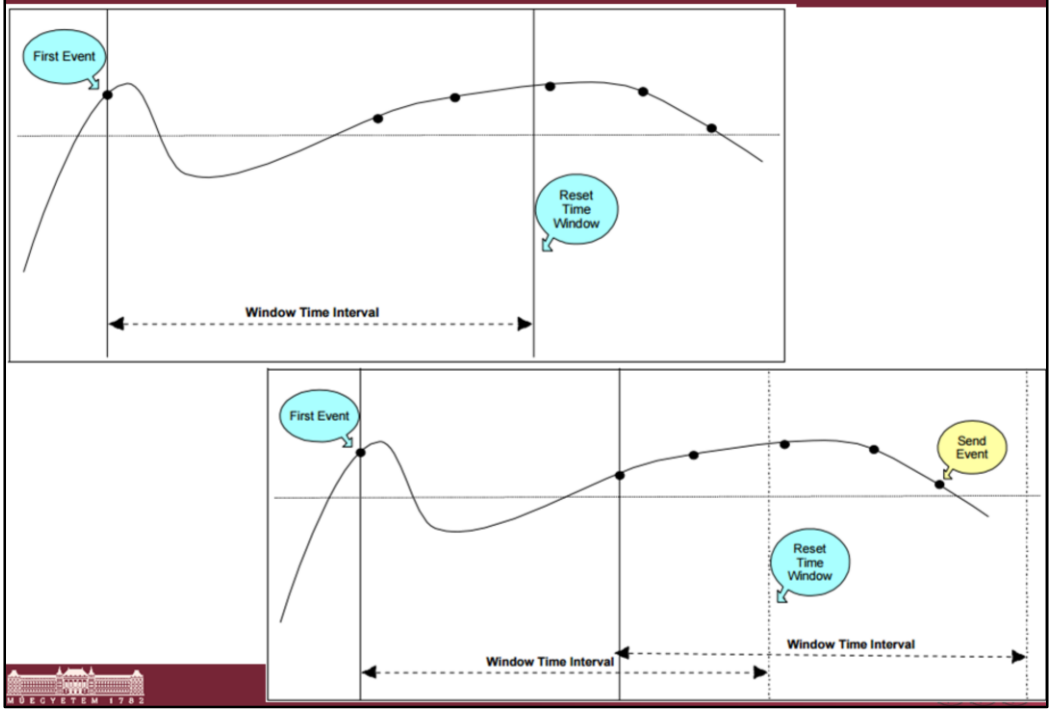
- *Azon események felderítése és kezelése, amelyek ugyanannak a problémának ugyanazt a példányát reprezentálják.*

- A célok pont mint szűrésnél,
  - Feldolgozandó/továbbítandó adatmennyiség csökkentése
  - Redundáns információ eltávolítása
- De itt további tevékenységek

Throttling értelme: pl. a tranziens hibákat nem jelezzük, csak ha huzamosabb ideig fennáll a probléma
Statikus – csak az elsőnél értelmezett, dinamikus: mindig újraszámoljuk

Mikor nincs értelme a „Lassítás, aztán minden példánynak”? → Ha az elsőre úgyis reagálni kell
Ne küldjünk ki egy értesítést csak úgy „emlékeztetőül”, azzal csak nő az adatmennyiség

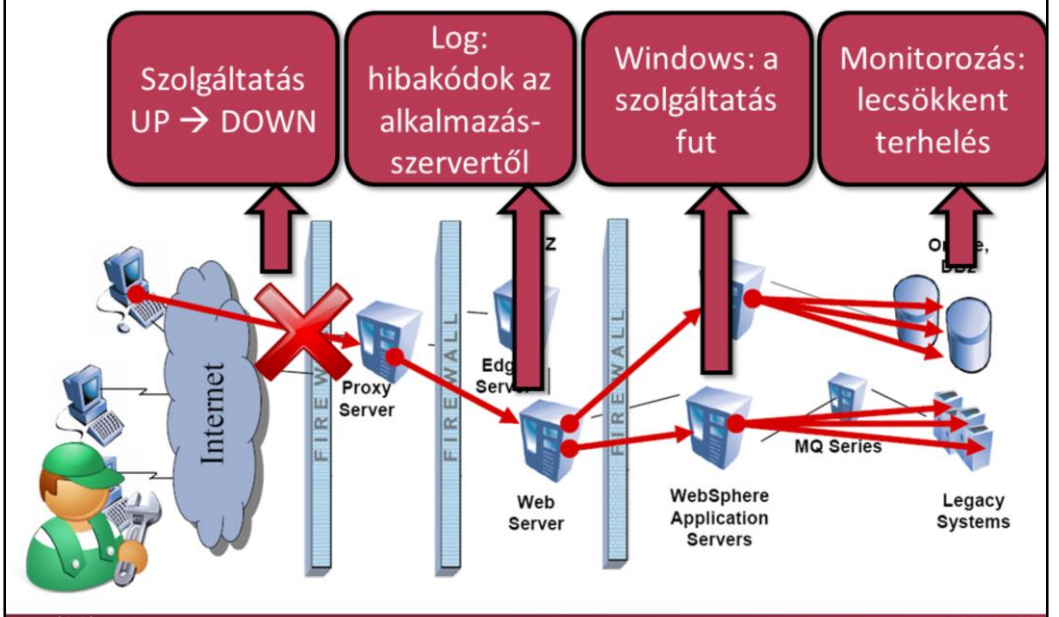
Statikus és dinamikus csúszóablak



Korreláció

- *Azonos probléma által generált vagy azonos erőforrásra vonatkozó események együttes kezelése*

Korreláció

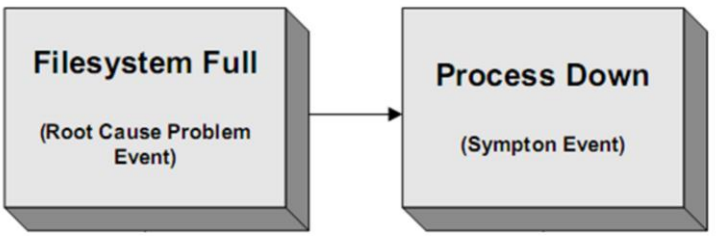

Szolgáltatás UP → DOWN
Log: hibakódok az alkalmazás-szervertől
Windows: a szolgáltatás fut
Monitorozás: lecsökkent terhelés
Internet
FIREWALL
Proxy Server
Web Server
WebSphere Application Servers
MQ Series
Legacy Systems

Korreláció

- *Azonos probléma által generált vagy azonos erőforrásra vonatkozó események együttes kezelése*
- Gyakran a hibadetektálás nem oldható meg egyetlen forrás vizsgálatával
- Itt a korreláció magát a tevékenységet jelöli

Korreláció típusok

- Kiváltó ok korreláció
  - ~ végigvezetni a fault-error-failure ágat → elég riasztanunk a kiváltó okkal és/vagy a szolgáltatási szintű hibahatással kapcsolatban
  - Elsődleges esemény – jelzi a kiváltó okot
  - Szimptóma esemény – jelzi a végeredményt

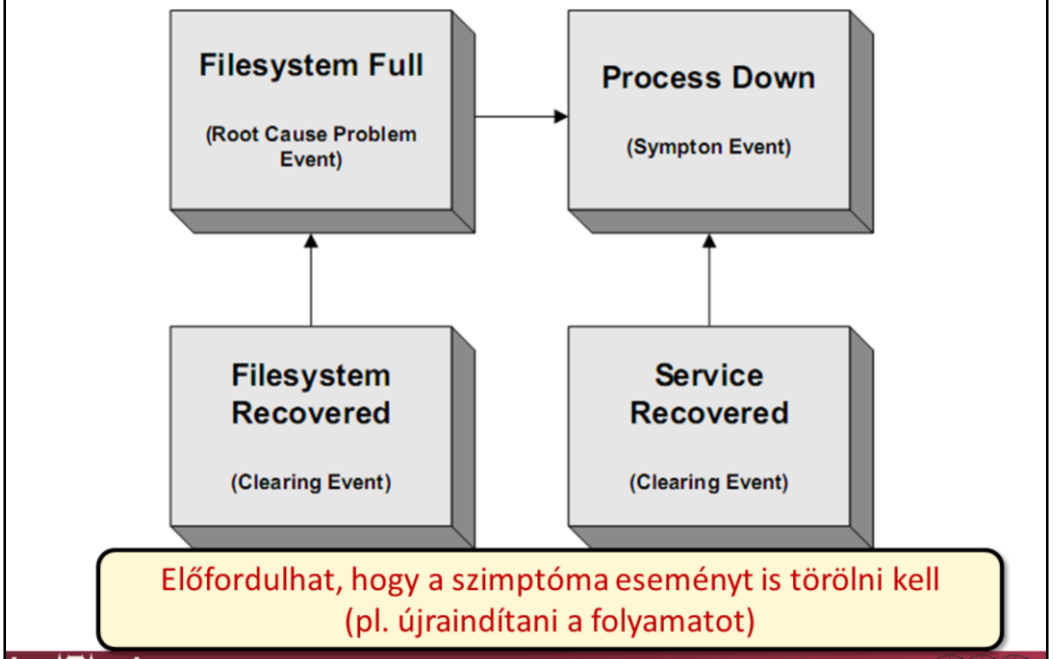


A cél: valami hierarchia kiépítése

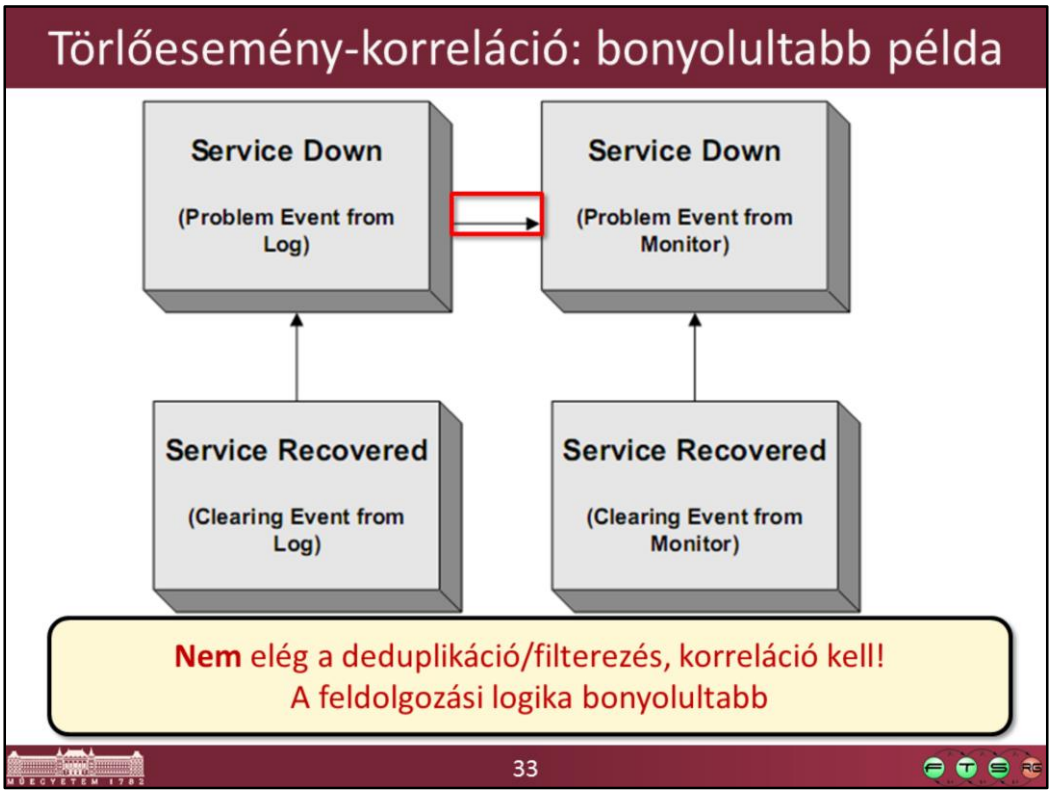
Korreláció típusok

- Törlőesemény korreláció
  - *Törlőesemény – az az esemény, amely a probléma esemény által jelzett problémát megszűntnek nyilvánítja.*
  - törlőesemény beérkezésekor az eredeti probléma eseményt lezárjuk (pl. töröljük).
- Tervezői döntés: mi történjen a szimptóma eseményekkel?

„Kiváltó ok” korreláció és törlőesemények



Előfordulhat, hogy a szimptóma eseményt is törölni kell
(pl. újraindítani a folyamatot)



Mi van, ha elrontottuk a filterezést?

Korreláció

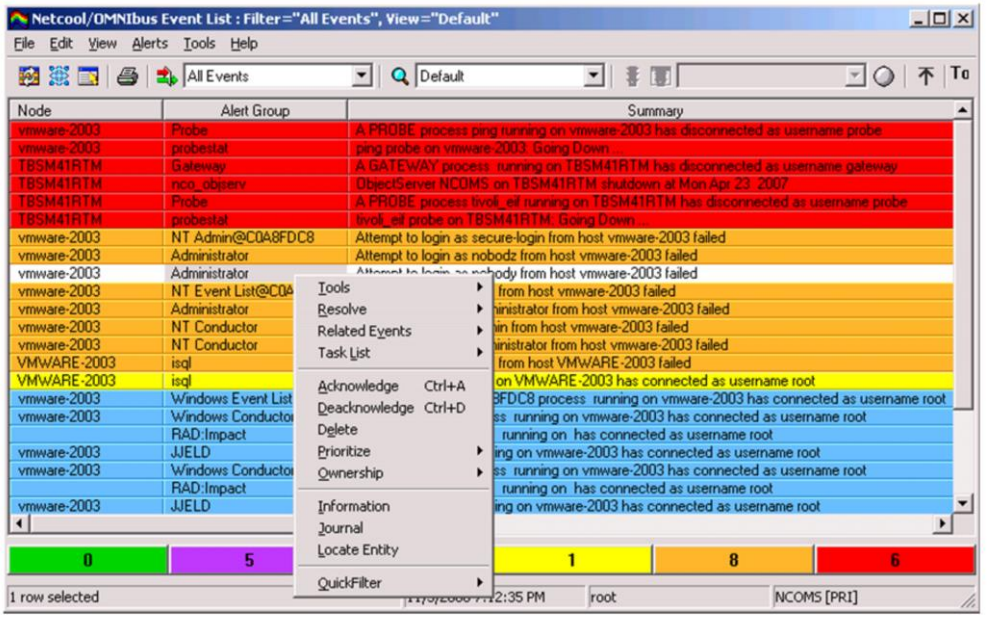
- Honnan tudjuk, hogy az események korreláltak?
  - Szakértői tudás
    - Topológia, konfiguráció, hibaterjedési mechanizmusok stb.
  - Automatikus felderítés
    - Asszociációs szabályok keresése → egy adott csúszóablakban mely események együttes előfordulása gyakori
- Mi történjen a duplikátumokkal?
  - Inkább az első esemény súlyosságát érdemes növelni
    - Esetleg csatoljuk a többi időbélyegét
    - A szinkronizáció könnyebb később
- Csúszóablak konfiguráció!

Esetleg használhatunk csúszóablakot, de akkor a primary eseményeket többszörözve kell kiküldenünk!

Értesítés

- *Az eseménykezelés lépései eredményeinek továbbítása/megjelenítése a megfelelő felhasználó felé*
- Megfelelő felhasználó
  - Process owner, help desk, adminisztrátorok
- Információs csatornák
  - Konzol, „paging”, e-mail, **ticketing rendszerbe** integrálás

Netcool/OMNIbus Event List



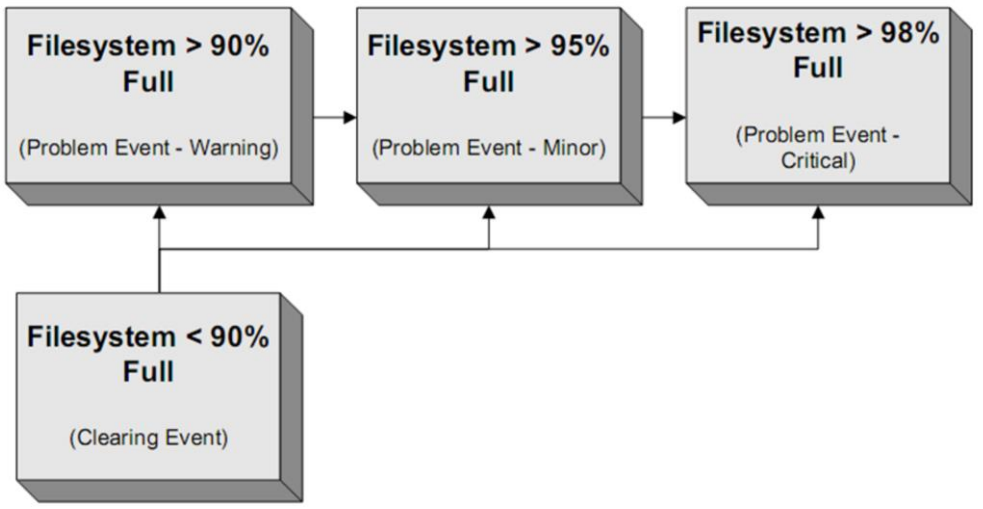
Eszkalálás

- *Az esemény súlyosság attribútumának módosítása a lehető legpontosabb információ továbbítása érdekében*
- Nem maradhatnak kezeletlen események
- Idővel ronthatják pl. a rendelkezésre állásunkat

Eszkalálás

- Ahelyett, hogy több eseményt küldenénk, módosítsuk a súlyosságot
- Általában felfelé ☺
  - Amiatt ne keletkezzen egy új esemény, hogy csökkent a helyzet súlyossága
- Elegendő egy törlőesemény ☺

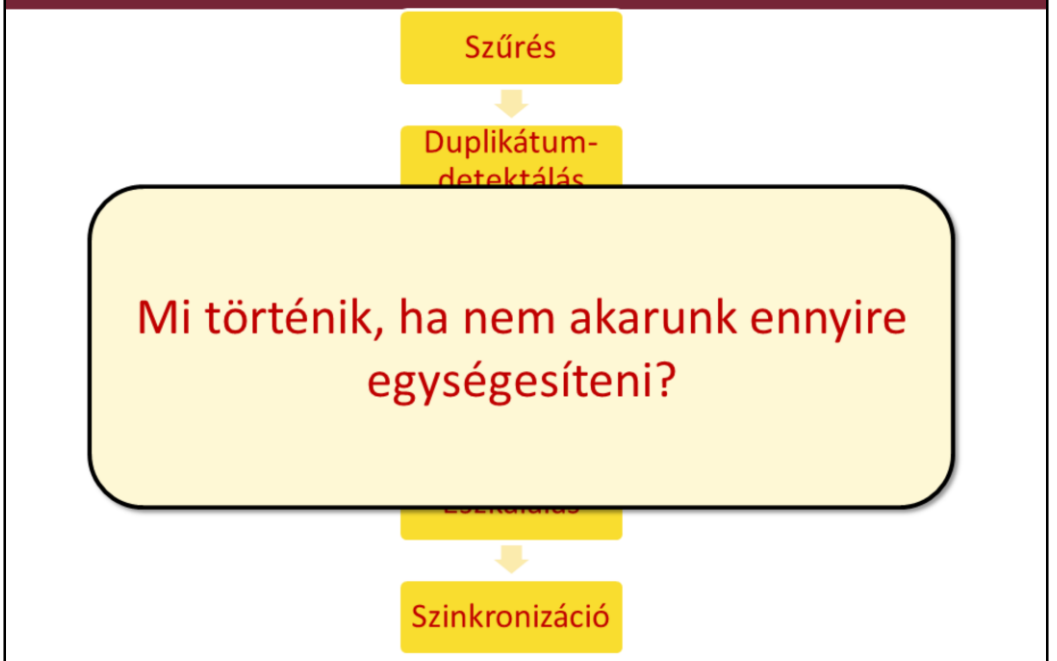
Esemény-eszkaláció és a törlőesemény



Szinkronizáció

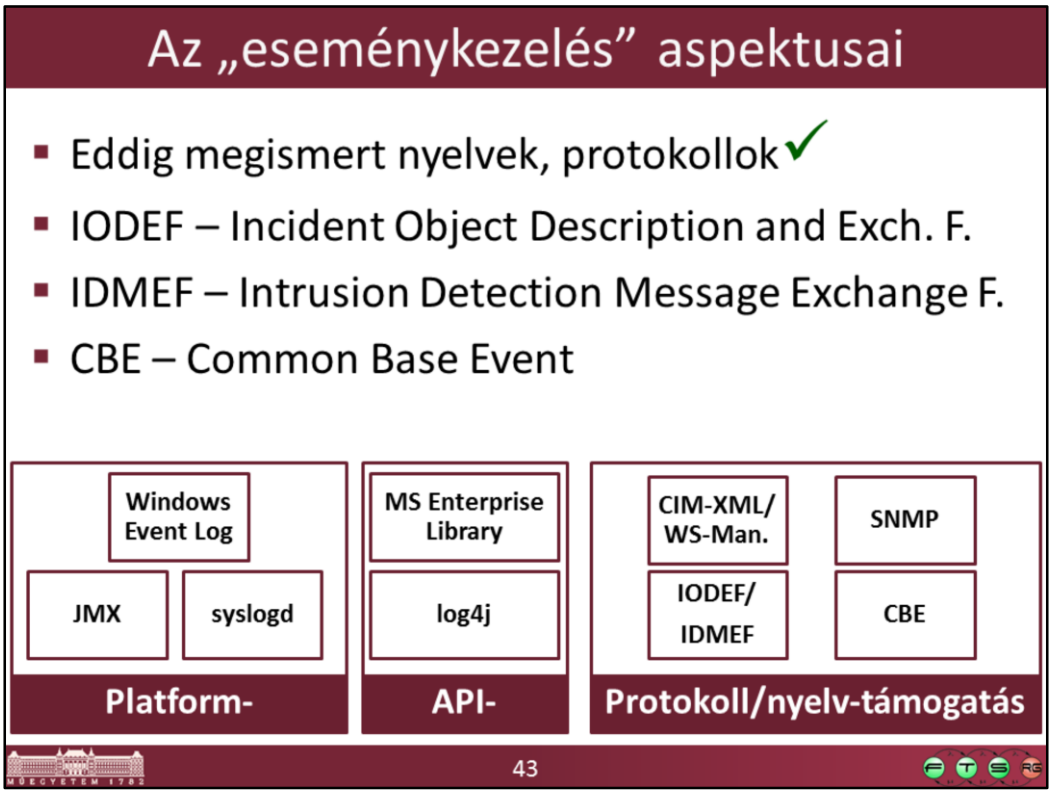
- *Annak biztosítása, hogy a különböző feldolgozó csomópontok a rendszer egy konzisztens állapotképét lássák*
- Kiemelten fontos a trouble-ticketing rendszerrel történő szinkronizáció

A feldolgozás jellemző lépései



Célvezérelt eseménykezelés?

- Adott rengeteg eseményforrás
  - Naplók, monitorozás, platform eseménykezelők, …
- Tfh. adott egy esemény-feldolgozó eszköz
  - Sok „enterprise” termék; de a F/OSS is alternatíva
- Tfh. adott a cél
  - Pl.: „proaktív hibahatás-elkerülés redundáns infrastruktúrán”
- Források és feldolgozás konfiguráció-tervezése
  - Tudnunk kell, mit honnan és milyen gyakran kérdezünk le, pontosan milyen konfigurációban
  - Default + „mérnöki tapasztalat” + egyszerű intelligencia + folyamatos csiszolás



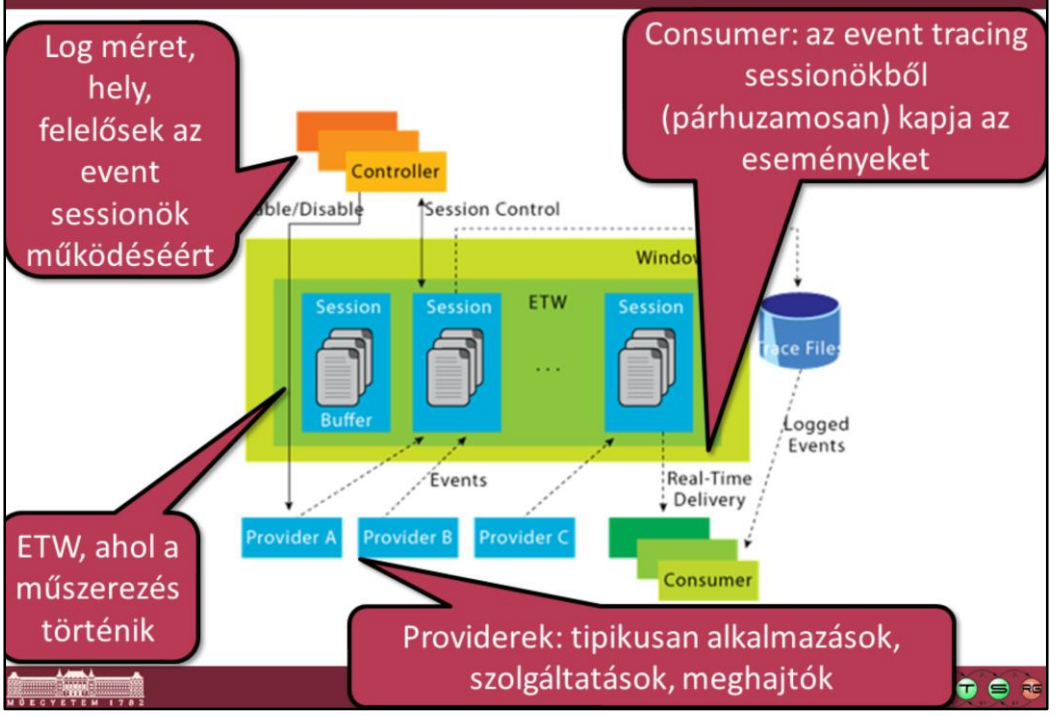
CBE – IBM Web Service Management implementáció

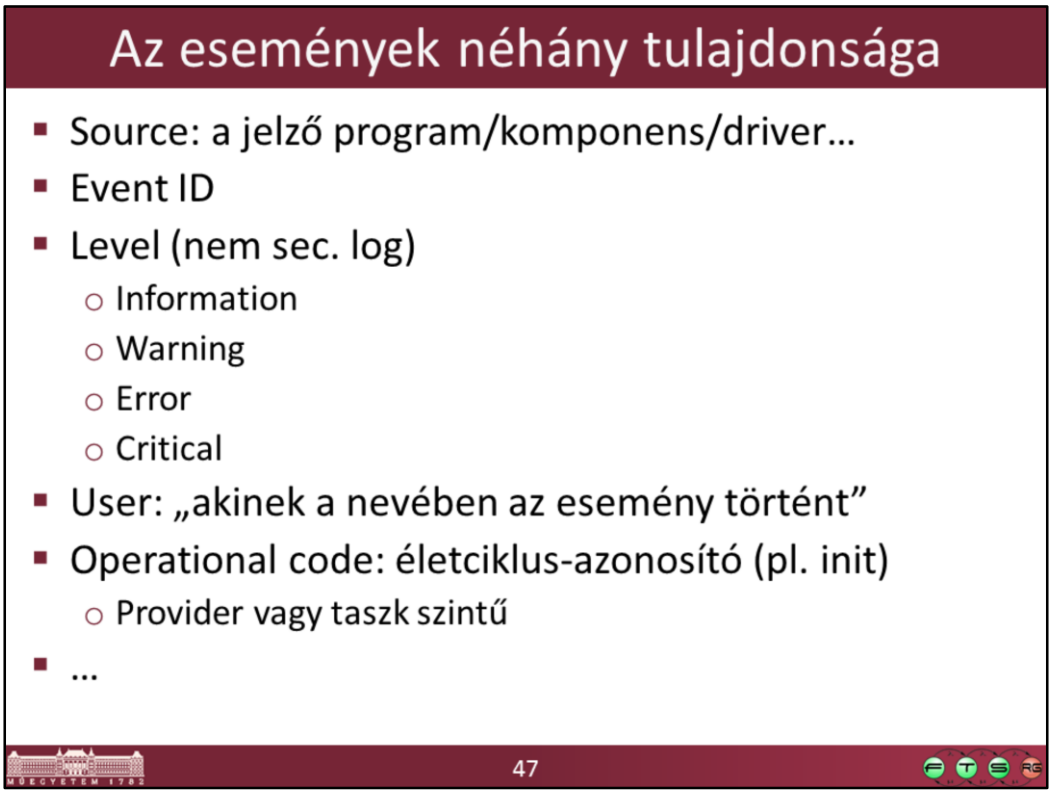
Windows Event Log

Windows Event Log

- Központosított helyi eseménynaplózás
  - Az eredeti NT óta (1993)
- Eredetileg három „log”
  - System
  - Application
  - Security
- Háttérben: naplóállományok
- Event Viewer: MMC snap-in
- Vista & Server 2008 - újraírt eseménykezelő architektúra: „Windows Event Log” (Eventing 6.0)

Event Trace for Windows

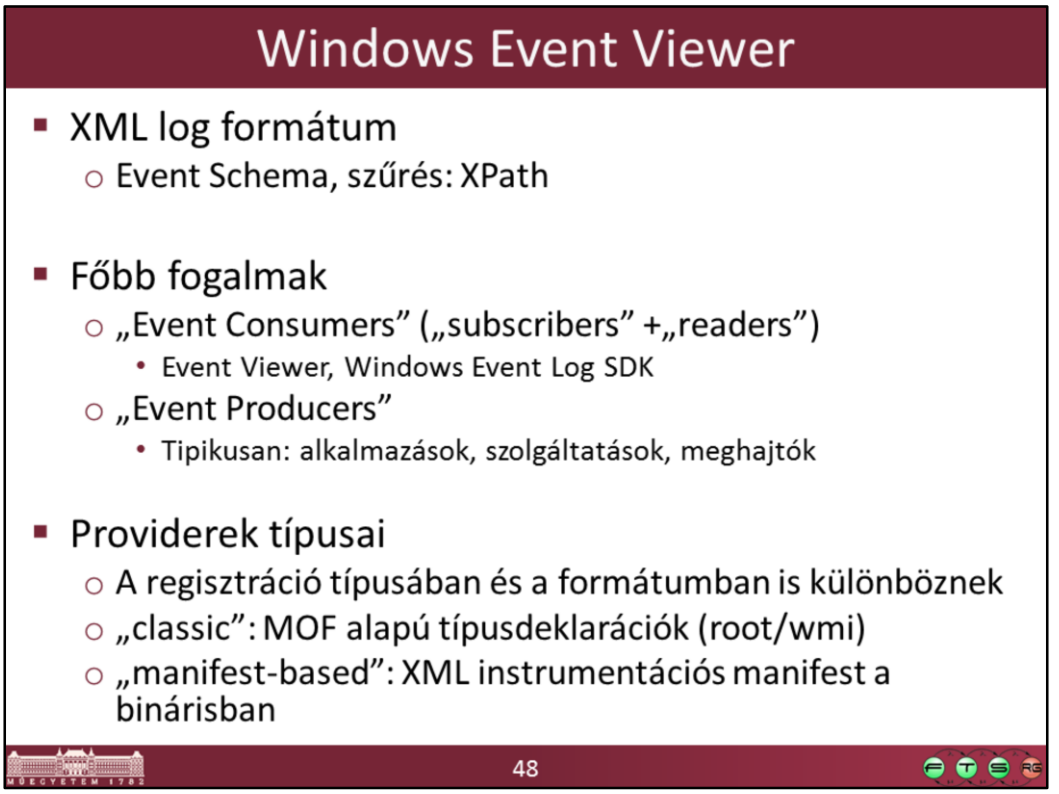




A help-ből:

Information. Indicates that a change in an application or component has occurred, such as an operation has successfully completed, a resource has been created, or a service started.
Warning. Indicates that an issue has occurred that can impact service or result in a more serious problem if action is not taken.
Error. Indicates that a problem has occurred, which might impact functionality that is external to the application or component that triggered the event.
Critical. Indicates that a failure has occurred from which the application or component that triggered the event cannot automatically recover.

Az eseménykezelés előadáson foglalkozunk még az események/logbejegyzések lehetséges kategorizálásaival; amit érdemes látni az az, hogy súlyossági osztályozás szempontjából nincsenek igazán nagy különbségek a különböző megközelítések között.

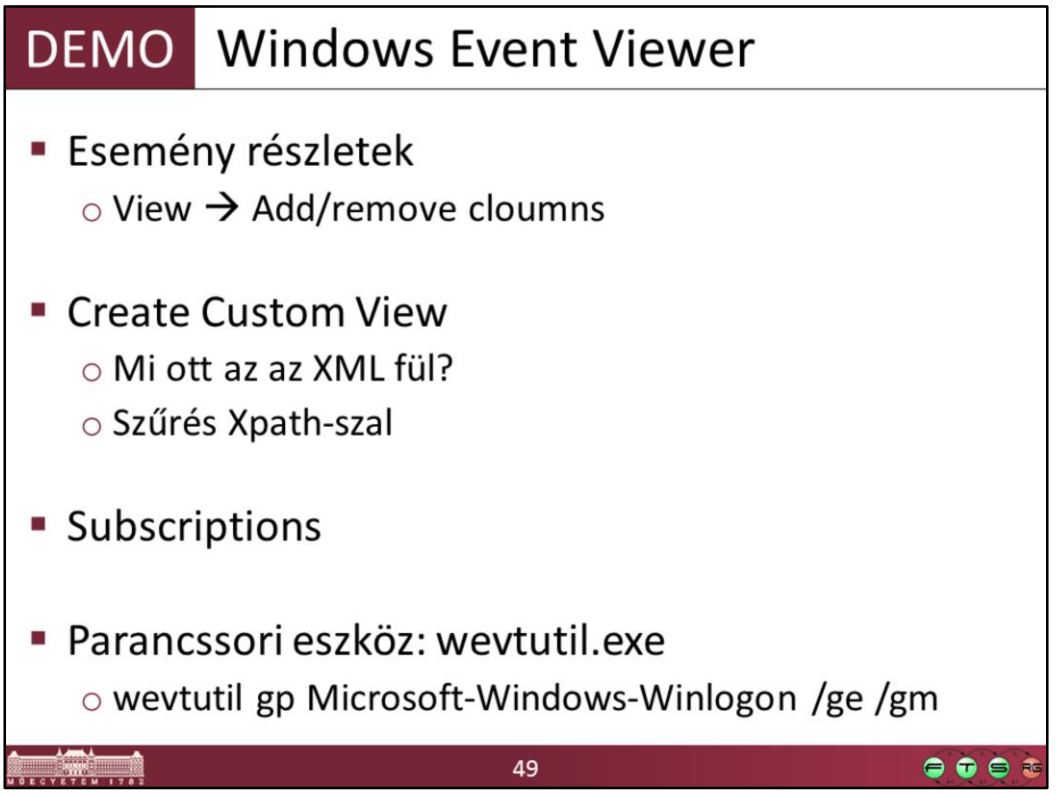


Xpath – XML Path Language, egy query nyelv XML dokumentumok csomópontjainak szűrésére

The MOF (Managed Object Format) file is a mechanism for expressing and registering the classes, providers, properties, and instances for a particular WMI repository implementation. Providers can use the MOF Compiler (MOFComp.exe) to add the classes to the WMI Repository.

1. Megírunk egy alkalmazást, abba beledobunk egy xml-t, amiben az összes provider információ benne van, ezt dobhatjuk tovább pl. az Event Tracingnek.

Event Tracing → Event Tracing for Windows (ETW) provides application programmers the ability to start and stop event tracing sessions, instrument an application to provide trace events, and consume trace events. Trace events contain an event header and provider-defined data that describes the current state of an application or operation. You can use the events to debug an application and perform capacity and performance analysis.

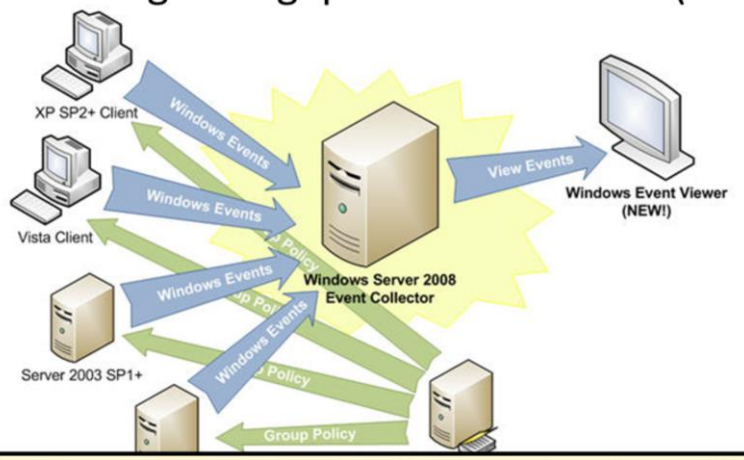


Demo: Windows 7. Az Eventing és az Event Viewer fejlődéséről egy jó rövid összefoglaló: http://en.wikipedia.org/wiki/Event_Viewer

Az Xpath tutorial: http://www.w3schools.com/XPath/default.asp).

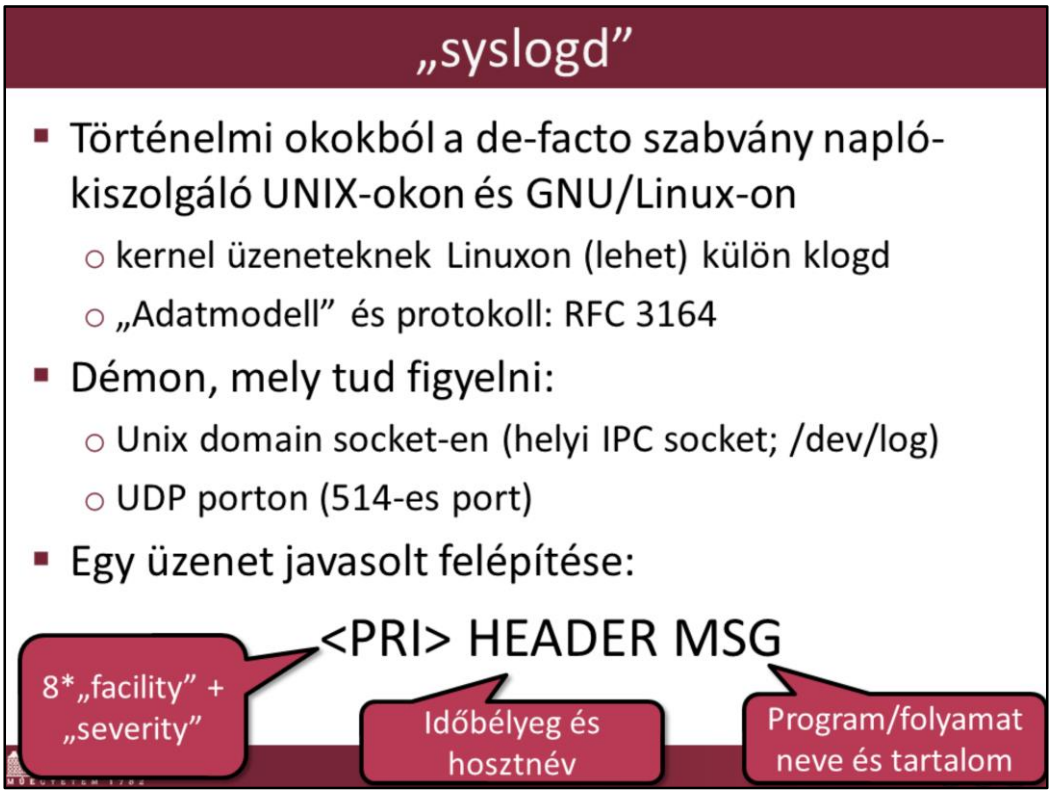
Esemény-továbbítás

- Lásd Event Viewer, Subscriptions
- WS-Eventing →célgépeken WinRM kell (WS-Man)



Már láttuk: „nehézsúlyú” eseménykezeléshez azért több kell

syslogd



Syslog – 80-as évek, Eric Allman, Sendmail részeként, később vette át a Unix közösség

Syslog Priority

- Általános formula: $8 \times$ „$facility$” $+$ „$severity$”
- Facility-k és súlyosságok ekkor pontosan hierarchizálva
- Facility-k száma: 24
- Severity-k száma: 8

RFC3164 „facility”-k

0: kernel messages
1: user-level messages
2: mail system
3: system daemons
4: security/authorization messages
5: messages generated internally by syslogd
6: line printer subsystem
7: network news subsystem
8: UUCP subsystem
9: clock daemon
10: security/authorization messages (note 1)
11: FTP daemon
...

...23-ig. Figyelem: az egyes implementációk sokszor nem felelnek meg ennek

RFC3164 „severity”-k

0 - Emergency: system is unusable

1 - Alert: action must be taken immediately

2 - Critical: critical conditions

3 - Error: error conditions

4 - Warning: warning conditions

5 - Notice: normal but significant condition

6 - Informational: informational messages

7 - Debug: debug-level messages

DEMO Syslogd + logger

- `/etc/syslog.conf`
- `logger -p cron.1 "Hello world"`
- `tail /var/log/cron`

/etc/syslog.conf

```
#kern.*                                         /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none        /var/log/messages

# The authpriv file has restricted access.
authpriv.*                                      /var/log/secure

# Log all the mail messages in one place.
mail.*                                          -/var/log/maillog


# Log cron stuff
cron.*                                          /var/log/cron

# Everybody gets emergency messages
*.emerg                                         *
```

File, udp, named pipe, terminál…

Néhány probléma a syslog-gal

- Inkompatibilis megvalósítások
- Csak facility és severity alapján válogatás
  - Démonok?
- Rossz dátumformátum
- UDP!
- Max. 1024 byte
- Általában root-ként fut
- …

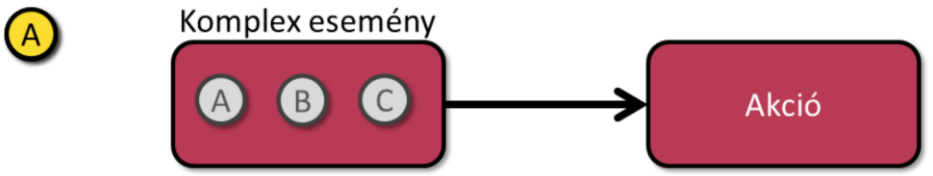
Viszont valamennyire „közös nevező”

Felhasznált forrás: https://unixlinux.tmit.bme.hu/Naplózás

„KOMPLEX ESEMÉNYEK” FELDOLGOZÁSA

Motiváció

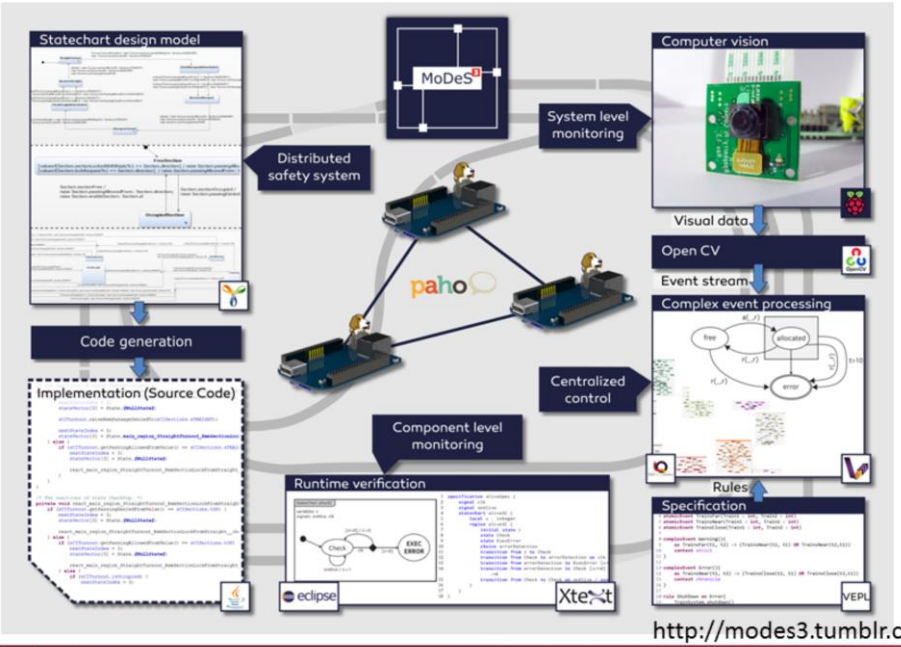
- Esemény-feldolgozás alapja: a mintafelismerés
  - Az érdekes események összetettek lehetnek
- Komplex esemény: elemi eseményekből álló struktúra
  - Complex Event Processing – CEP
- Példák
  - *„A webszerver terheltsége 90% és az adatbázis szerveren lekérdezést futtatnak.” ⇨ „Vonjunk be tartalék erőforrást.”*
  - *„Az X részvények értéke jelentősen csökkent, és a vele korreláló Y részvények is elkezdtek esni.” ⇨ „Adjunk el Y részvényeket.”*



CEP alkalmazási területek

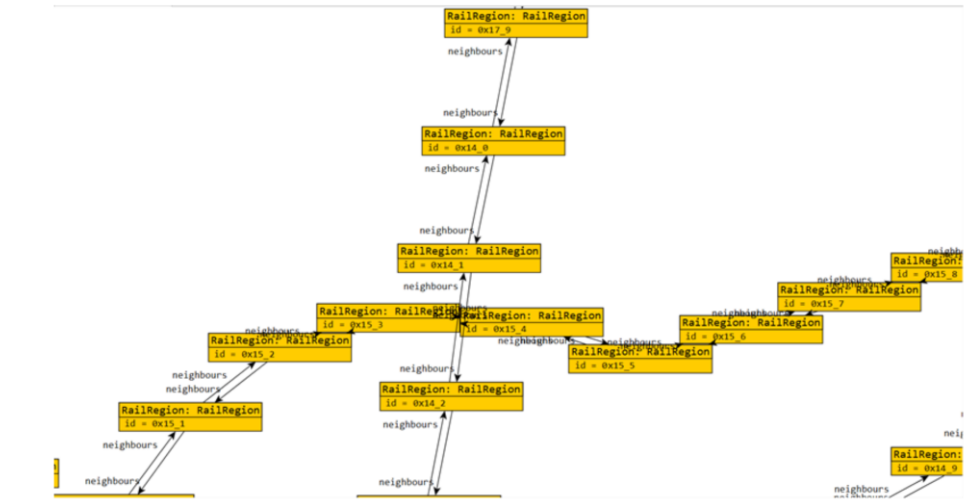
- **Nagy IT rendszerek üzemeltetése**
  - **Komplex támadások felderítése**
  - **Metrika kiértékelés**
- Internet of Things / Cyber-Physical Systems
  - Szenzoradatok feldolgozása
- Üzleti alkalmazások
  - Tőzsde, befektetések
  - Hitelek árazása
- Online visszaélések felderítése/megelőzése
  - Gyanús tranzakciók ellenőrzése
  - Fogadási adatok elemzése (pl. UEFA)
- Biztonságtechnika
  - Pl. dDOS ellen

Esettanulmány: MODES3



http://modes3.tumblr.com/

MODES3: komplex események



Linkek – Windows eseménykezelés

- Rövid áttekintés a Windows eseménykezelésről
  - http://msdn.microsoft.com/en-us/library/aa382610(VS.85).aspx
  - http://en.wikipedia.org/wiki/Event_Viewer
- Windows Event Forwarding (Eventing 6):
  - http://blogs.technet.com/otto/archive/2008/07/08/quick-and-dirty-enterprise-eventing-for-windows.aspx
- Windows Event Log – fejlesztői áttekintés
  - http://msdn.microsoft.com/en-us/library/bb756956.aspx
- Érdeklődőknek (érdekes olvasmány):
  - http://www.dfrws.org/2007/proceedings/p65-schuster.pdf

Linkek - syslog

- Syslog áttekintés
  - http://en.wikipedia.org/wiki/Syslog
- RFC 3164
  - http://www.ietf.org/rfc/rfc3164
- „The Ins and Outs of System Logging Using Syslog”
  - http://www.sans.org/rr/whitepapers/logging/1168.php
- Áttekintés a Linux/UNIX naplózásról
  - https://unixlinux.tmit.bme.hu//Naplózás

További linkek

- Event Management Best Practices (IBM redbook)
  - http://www.redbooks.ibm.com/abstracts/sg246094.html?Open
- Netcool/OMNIbus 7.2.1 Infocenter
  - http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.netcool_OMNIbus.doc_7.2.1/welcome.htm