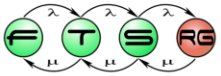
Intelligens rendszerfelügyelet (VIMIA370)

Eseménykezelés

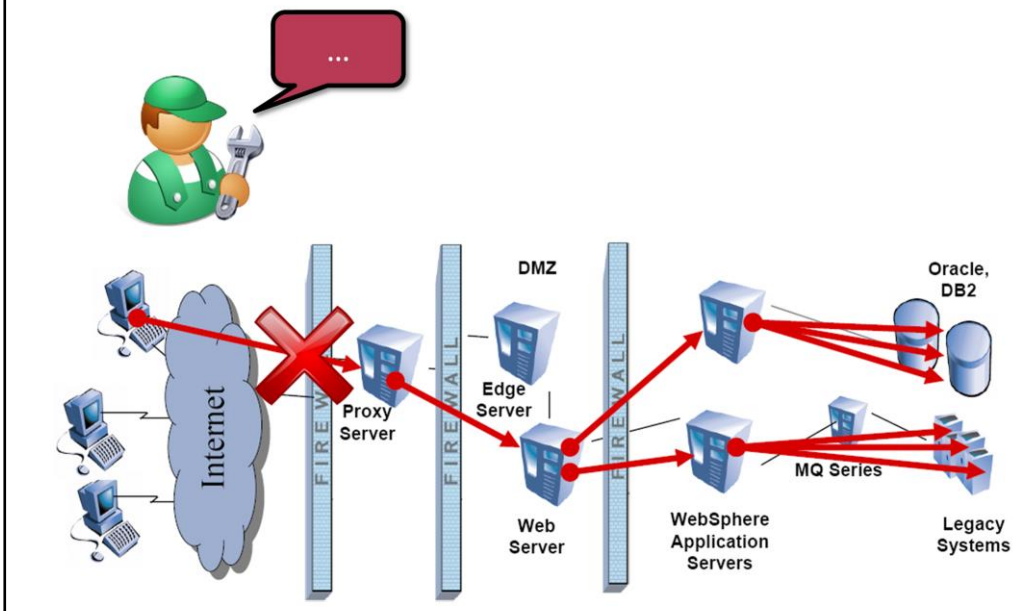
Kocsis Imre
http://mit.bme.hu/~ikocsis/



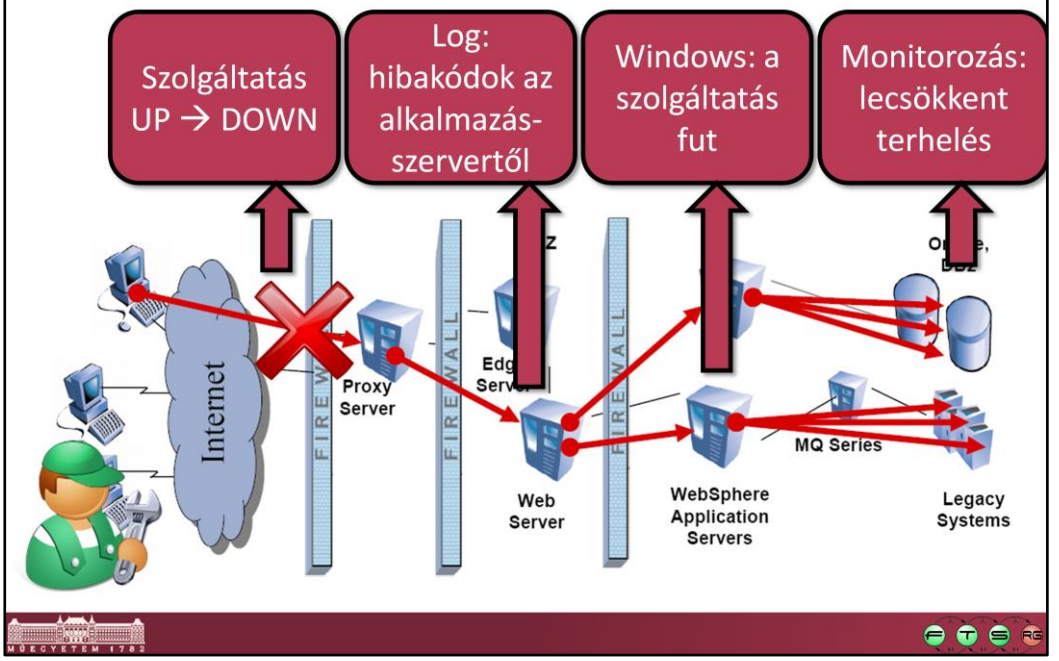
Budapesti Műszaki és Gazdaságtudományi Egyetem
Méréstechnika és Információs Rendszerek Tanszék

Utolsó módosítás: 2013.04.22

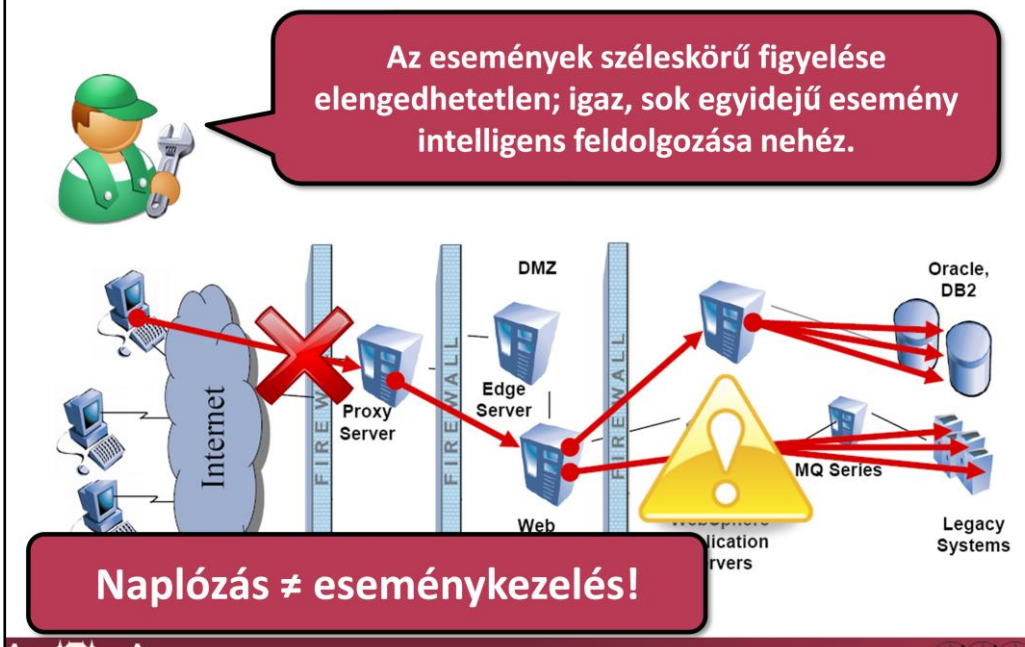
Motiváció


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

Az „esemény” fogalma

- Az IT szolgáltatás- és rendszerfelügyeletben az **esemény** olyan **adat**, ami egy vagy több **erőforrás**ról, illetve **szolgáltatás**ról hordoz információt.
- Példák?
- További szűkítések nélkül sajnos tényleg csak ennyire általános definíció adható.

Jellemző események egy IT infrastruktúrában

- Rendszerkomponensek működési mód- és állapotváltásai
  - Warning: DB2 has started ☺
  - Konfiguráció megváltozása
  - …
- Komponens szolgáltatásának végrehajtása
  - Apache access log
  - Új felhasználó került felvételre
  - …

Jellemző események egy IT infrastruktúrában

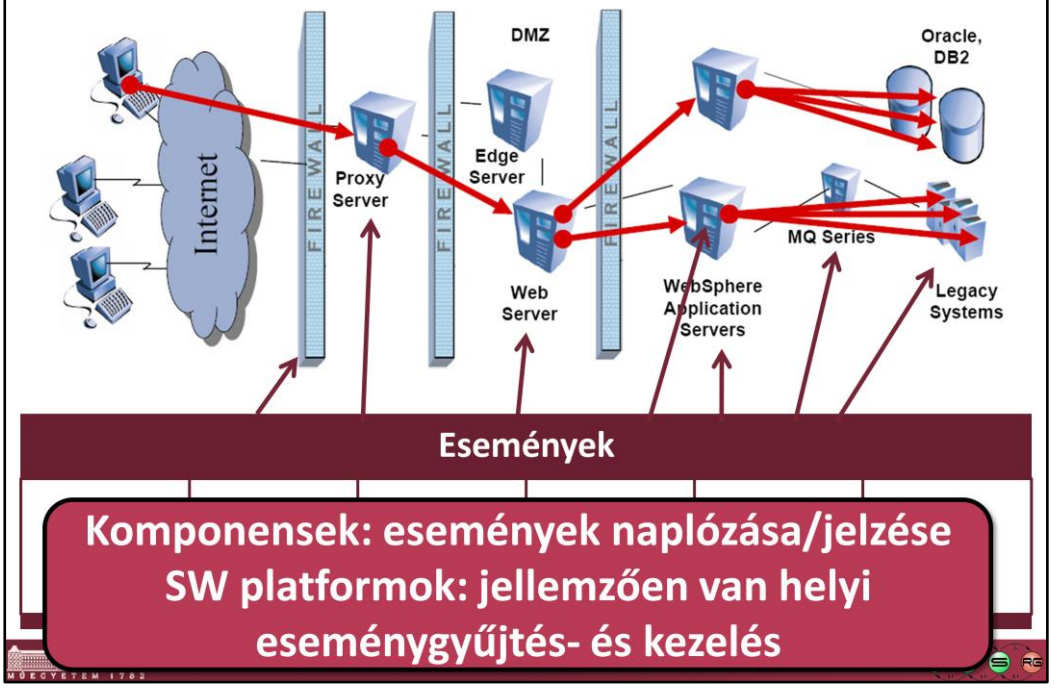
- Egy komponensen értelmezett metrikák megváltozása, vagy küszöbérték-átlépése
  - Web szerver lecsökkent válaszideje
  - Túl magas processzorhasználat
  - Szolgáltatás túl alacsony rendelkezésre állása
  - …
- Sokszor önmagában egy adott érték („mérés”)
  - N.B. az ilyesmi azért erőltetett

Jellemző események egy IT infrastruktúrában

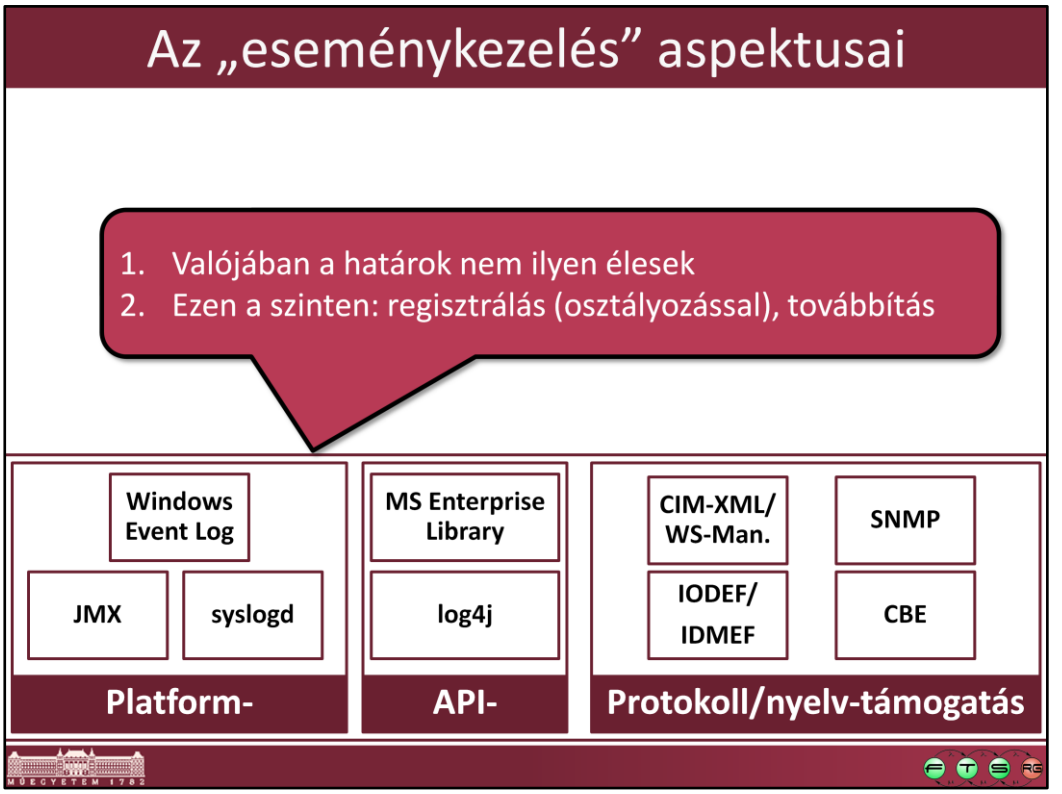
- Adatbiztonsági események
  - Sebezhetőség megjelenése
  - Támadási kísérlet
  - Bizalmasság, integritás vagy rendelkezésre állás sérülése
- Service Level Agreement-ek eseményei
  - SLA megsértése (SLA breach)
  - SLA-sértés köz
  - …

A felsorolás nyilván folytatható. (Sokáig.)

Események egy IT infrastruktúrában



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



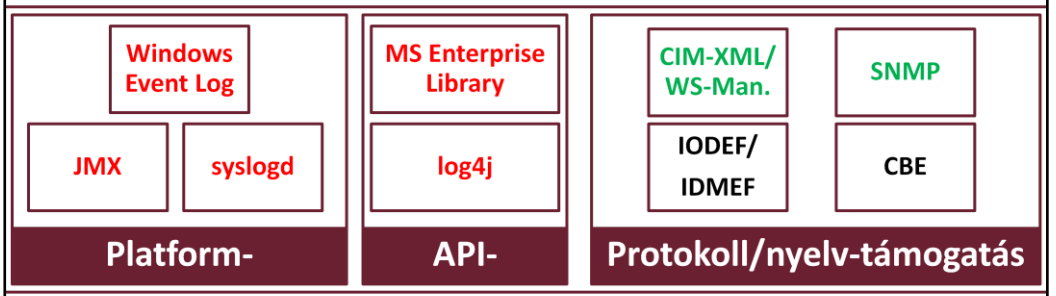
A JMX eseménykezelést valószínűleg röviden tárgyalni fogjuk a JMX-nél; a syslogd és a Windows Event Log ezen előadás anyaga.

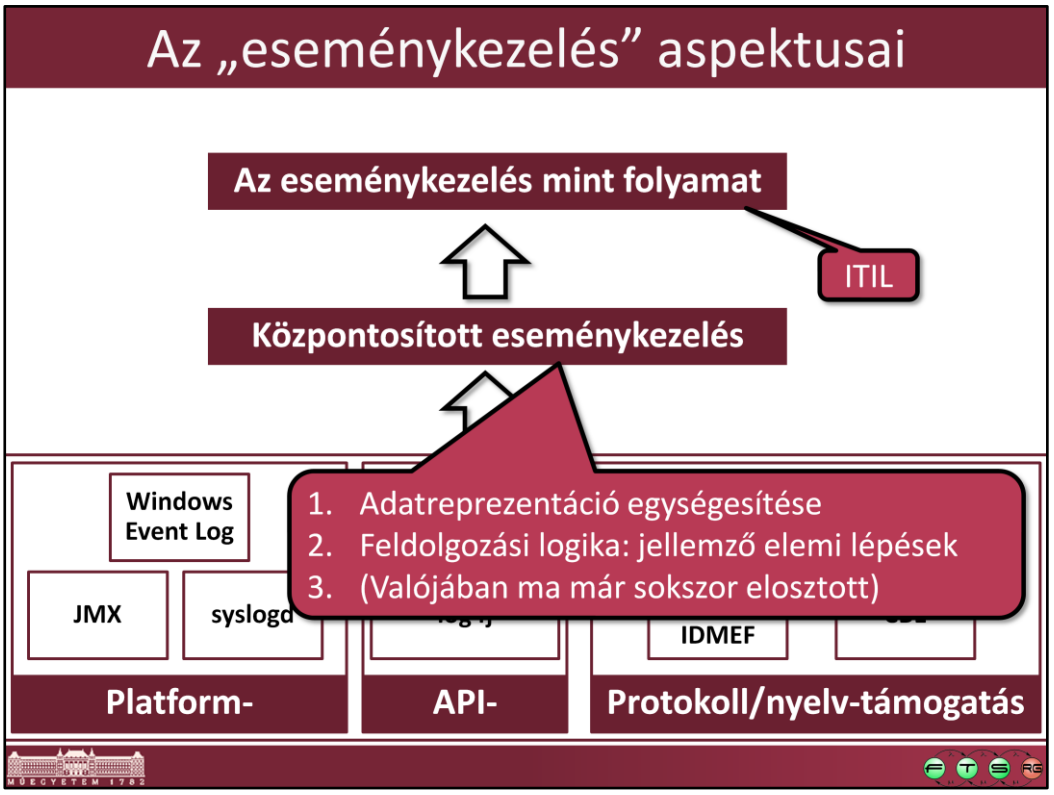
A Microsoft Enterprise Library („a set of tools and programming libraries for the Microsoft .NET Framework”) „Logging Application Block”-ja ad loggolást támogató API-t és mechanizmusokat; ez sokban hasonlít pl. a log4j-re a Java világból. Ezeket külön is fogjuk tárgyalni.

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 „eseménykezelés” aspektusai





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.

Windows Event Log

Windows Event Log

- Központosított helyi eseménynaplózás
  - Az eredeti NT óta (1993)
- Eredetileg három „log”
  - System
  - Application
  - Security
- Háttérben: naplóállományok (NT 6-ig: ~300 MB max)
- Event Viewer: MMC snap-in
- Vista & Server 2008 - újraírt eseménykezelő architektúra: „Windows Event Log” (Eventing 6.0)

Az események néhány tulajdonsága

- Source: a jelző program/komponens/driver…
- Event ID
- Level (nem sec. log)
  - Information
  - Warning
  - Error
  - Critical
- User: „akinek a nevében az esemény történt”
- Operational code: életciklus-azonosító (pl. init)
  - Provider vagy taszk szintű
- …

A help-ből:

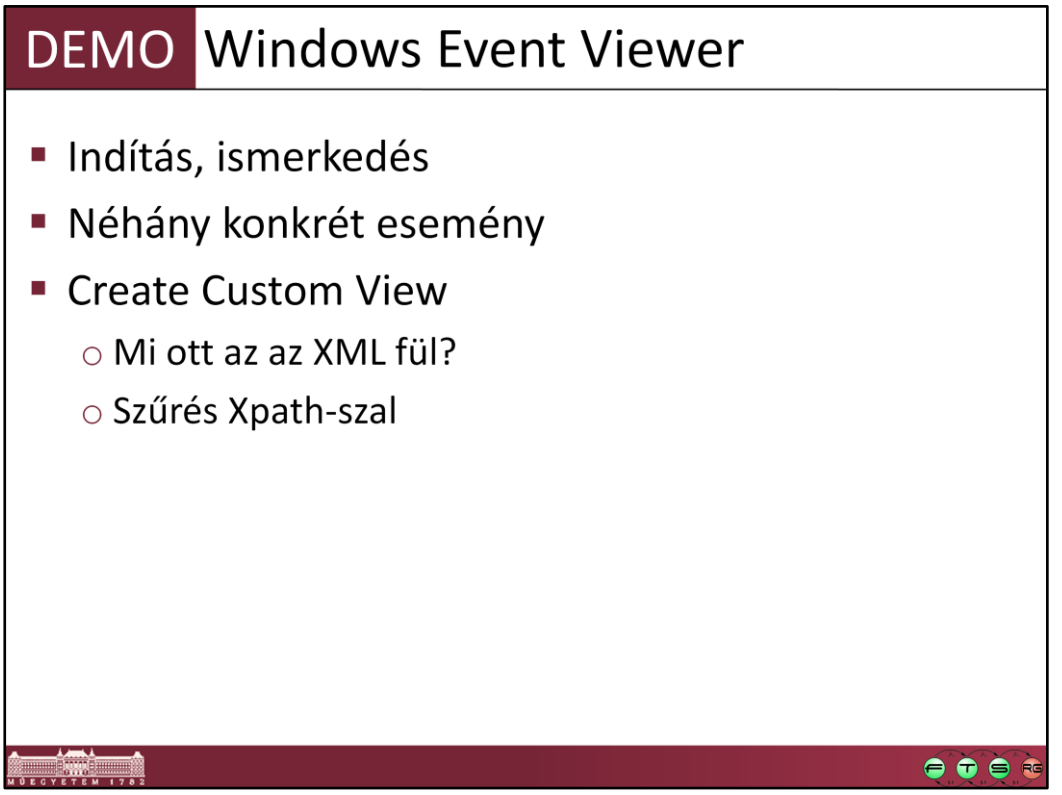
Information. Indicates that a change in an application or component has occurred, such as an operation has successfully completed, a resource has been created, or a service started.

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.



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

Az XPath-t nem ismerők számára highly recommended utánanézni (tutorial: http://www.w3schools.com/XPath/default.asp).

Windows Event Viewer

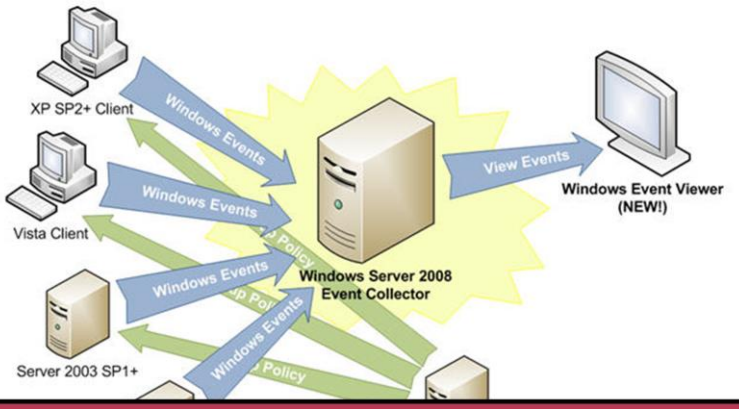
- XML log formátum
  - Event Schema, szűrés: XPath

További alapfogalmak: következő előadás

- Főbb fogalmak
  - „Event Consumers” („subscribers” +„readers”)
    - Event Viewer, Windows Event Log SDK
  - „Event Producers”
    - Tipikusan: alkalmazások, szolgáltatások, meghajtók
- Provider-ek
  - „classic”: MOF alapú típusdeklarációk (root/wmi)
  - „manifest-based”: XML instrumentációs manifest a binárisban
- Parancssori eszköz: wevtutil.exe
  - wevtutil gp Microsoft-Windows-Winlogon /ge /gm

Esemény-továbbítás

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

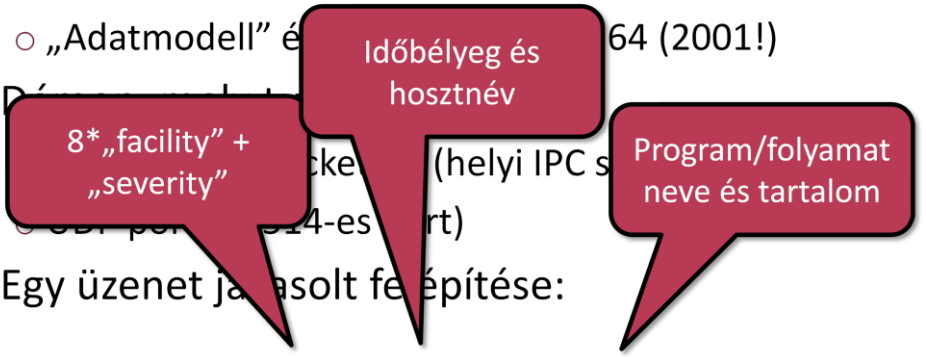


„Nehézsúlyú” eseménykezeléshez azért több kell

syslogd

„syslogd”

- Történelmi okokból a de-facto szabvány napló-kiszolgáló UNIX-okon és GNU/Linux-on
  - kernel üzeneteknek Linuxon (lehet) külön klogd
  - „Adatmodell” é 64 (2001!)
- D
  - cke (helyi IPC s
  - 4-es rt)
- Egy üzenet ja asolt fe építése:



PRI HEADER MSG

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

/etc/syslog.conf

-file
-udp
-named pipe
-terminál

```
                                                /dev/console

                    ot mail) of level info or higher.
                    authentication messages!
                    npriv.none;cron.none        /var/log/messages

                    has restricted access.
                                                /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                                         *
```

Példa: /var/log/secure

```
Mar  8 06:15:32 pegasus gdm[5577]: pam_unix(gdm:session): session
opened for user root by (uid=0)
Mar 11 14:56:51 pegasus gdm[5577]: pam_unix(gdm:session): session
closed for user root
Mar 11 14:57:01 pegasus gdm[5577]: pam_unix(gdm:auth):
authentication failure; logname= uid=0 euid=0 tty=:0 ruser= rhost=
user=ikocsis
Mar 11 14:57:09 pegasus gdm[5577]: pam_unix(gdm:session): session
opened for user root by (uid=0)
Mar 18 10:58:46 pegasus userhelper[7566]:
pam_timestamp(pirut:session): updated timestamp file
`/var/run/sudo/root/unknown'
Mar 18 10:58:46 pegasus userhelper[7569]: running '/usr/sbin/pirut'
with root privileges on behalf of 'root'
```

DEMO Syslogd + logger

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

Néhány probléma a syslog-gal

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

Viszont valamennyire „közös nevező”

Egyébként: mi van a saját naplót használó alkalmazásokkal?

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

Eseménykezelés

Esemény-feldolgozás

- Események gyűjtése é
  feldolgozása rendszer
- Eseményforrások és eseményfeldolgozók
  - Feldolgozók olgozási hierarchia

A folyamat-vetület az idén kimarad

Eseményfolyam + állapotok

„Eseményfolyam”
(event stream)

Alternatív modell: „esemény-felhő”

- Loggolás: az események immutábilisak
- Eseményfeldolgozás:
  - „alert” szemantika (→ megszűnhet)
  - módosítható állapot/tulajdonságok
    - lezárás, szelektív törlés, „elnyomás”…

A feldolgozás jellemző lépései

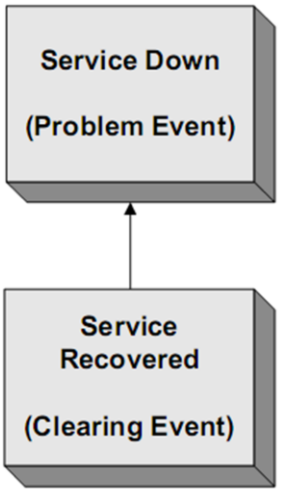
- Szűrés (filtering)
  - Erőforrás-kímélés: mind humán, mind IT
- Továbbítás (forwarding)
- „Lassítás” (throttling)
  - Túl magas CPU használat csak akkor érdekes, ha sokáig fennáll
- Duplikátumok detektálása (duplicate detection)
  - Ugyanaz többször (esetleg több forrásból)
- Elévültetés
- Korreláció: azonos probléma által generált / azonos erőforrásra vonatkozó események együttes kezelése

Lásd „Event Management Best Practices” (IBM Redbook SG24-6094):

1.3.2 Filtering and forwarding
1.3.3 Duplicate detection and throttling
1.3.4 Correlation

Korreláció: ügyeljünk arra, hogy valójában a *korreláció tényének felismerése* és a *korrelált eseményeken elvégzendő tevékenység* logikailag két egymást követő tevékenység, bár a fenti definíció kissé félrevezető ilyen szempontból.

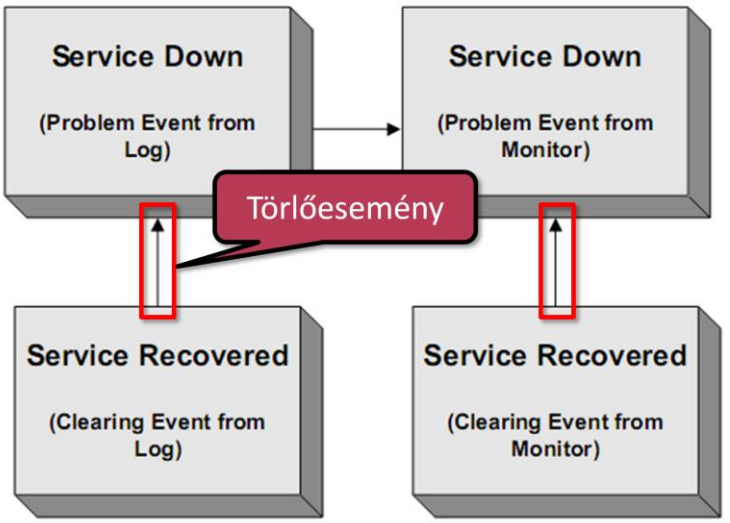
Korreláció: probléma- és törlőesemény



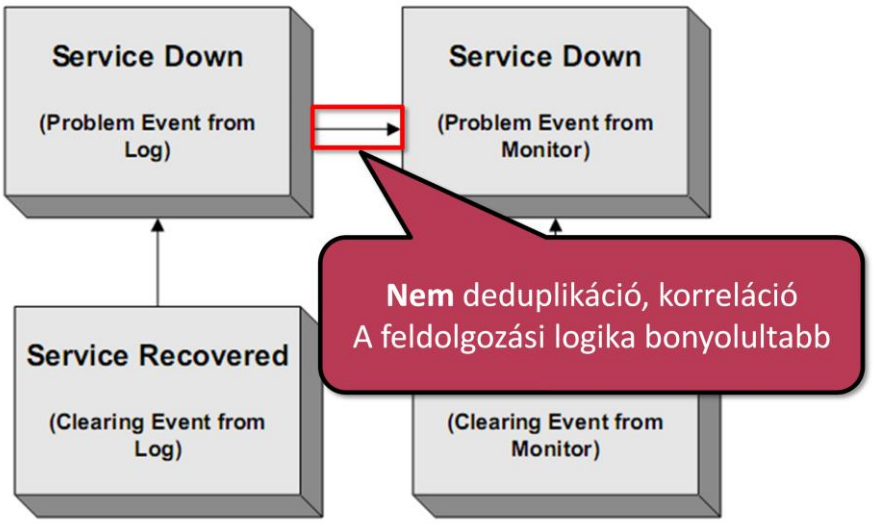
„Clearing event” beérkezésekor az eredeti „Problem event”-et általában *lezárjuk*; egyszerűbb esetben töröljük (bár ez sérthet auditálhatósági követelményeket).

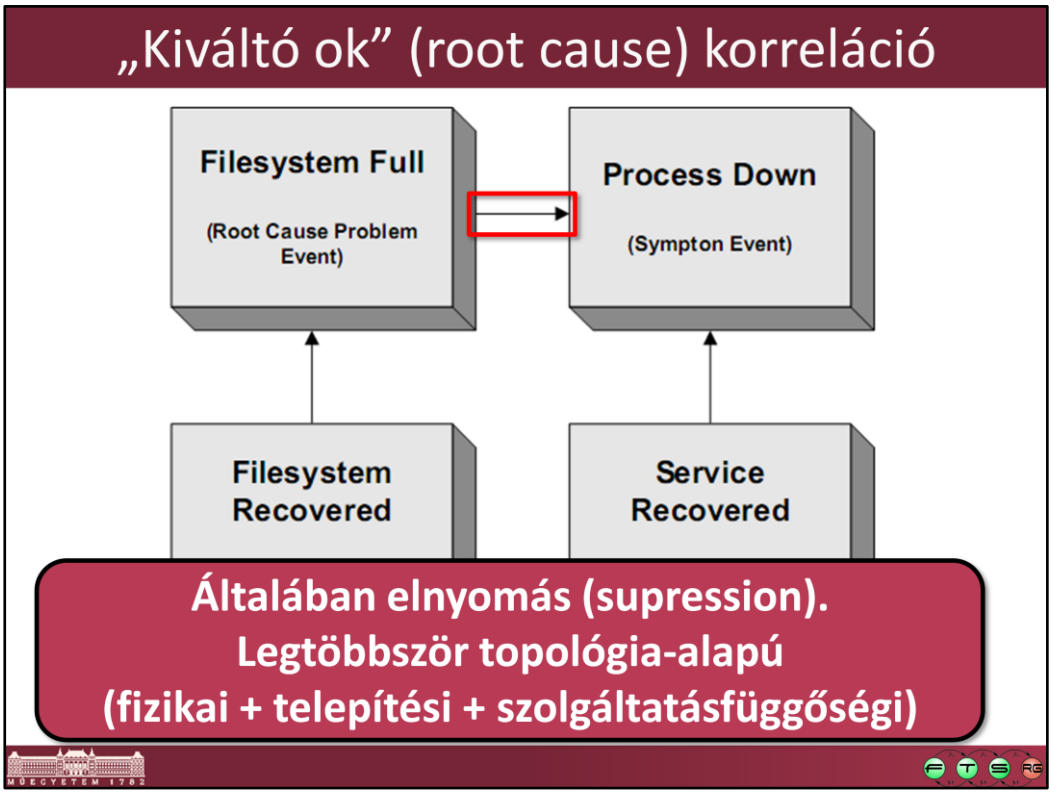
Azaz a kontextustól függ, hogy a probléma + törlőesemény korrelációs kapcsolatban lévő eseményeken milyen műveletet végzünk; ennél a korrelációs kapcsolatnál a lezárás és a törlés a jellemző.

Törlőesemény-korreláció: bonyolultabb példa



Törlőesemény-korreláció: bonyolultabb példa

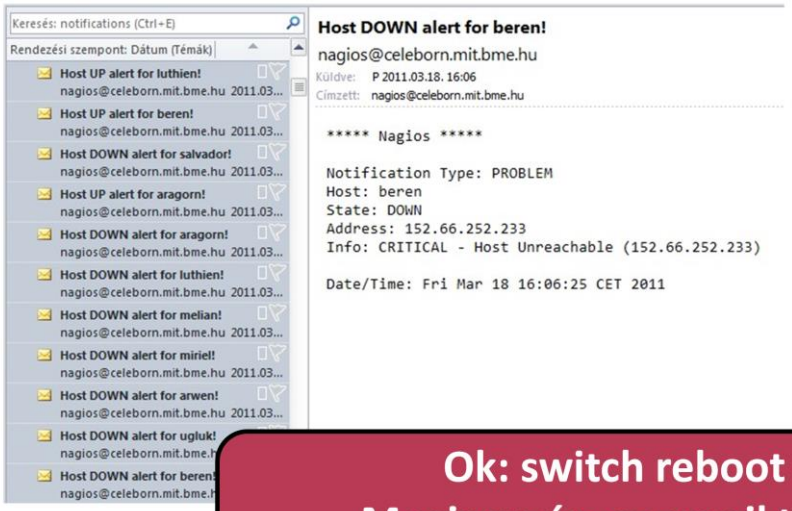




Megkülönböztetünk *elsődleges* eseményeket (root cause event / primary event) és szimptóma eseményeket (symptom event / secondary event). A kiváltó ok korreláció fő célja általában egy „elnyomási” (supression) hierarchia felállítása: általában elég riasztanunk a kiváltó okkal és/vagy a szolgáltatási szintű hibahatással kapcsolatban. A törlőeseményekkel kapcsolatban azonban vigyáznunk kell: egy elsődleges esemény megszűnte nem jelenti egy (az eredeti kontextusban) szimptóma megszűntét is! (Pl. a folyamatot lehet hogy újra kell indítani.)

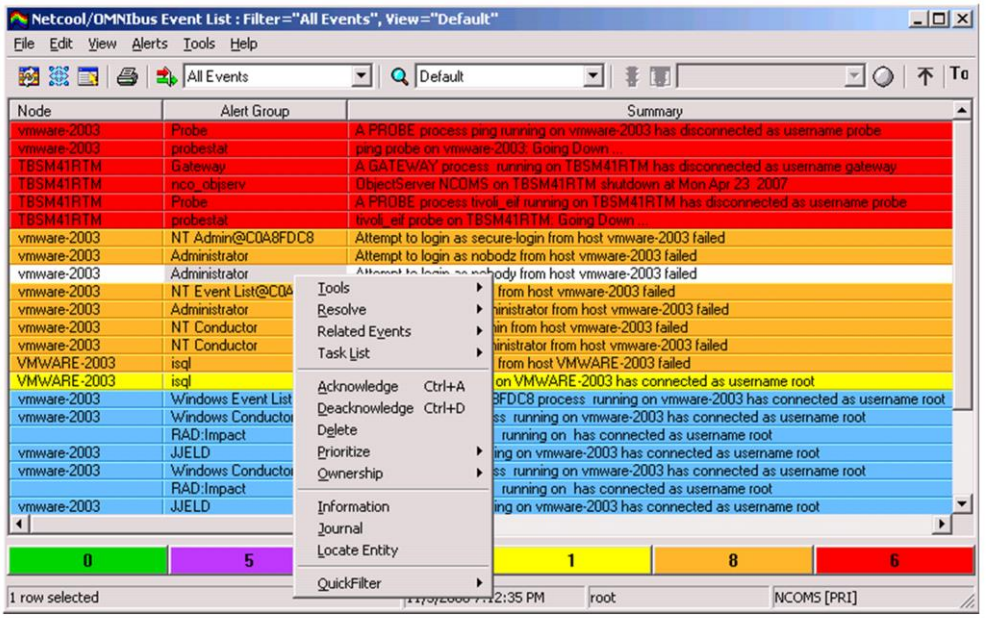
Btw. szerencsésebb az elsődleges esemény terminus technicus használata a kiváltó ok helyett.

„Event flood”

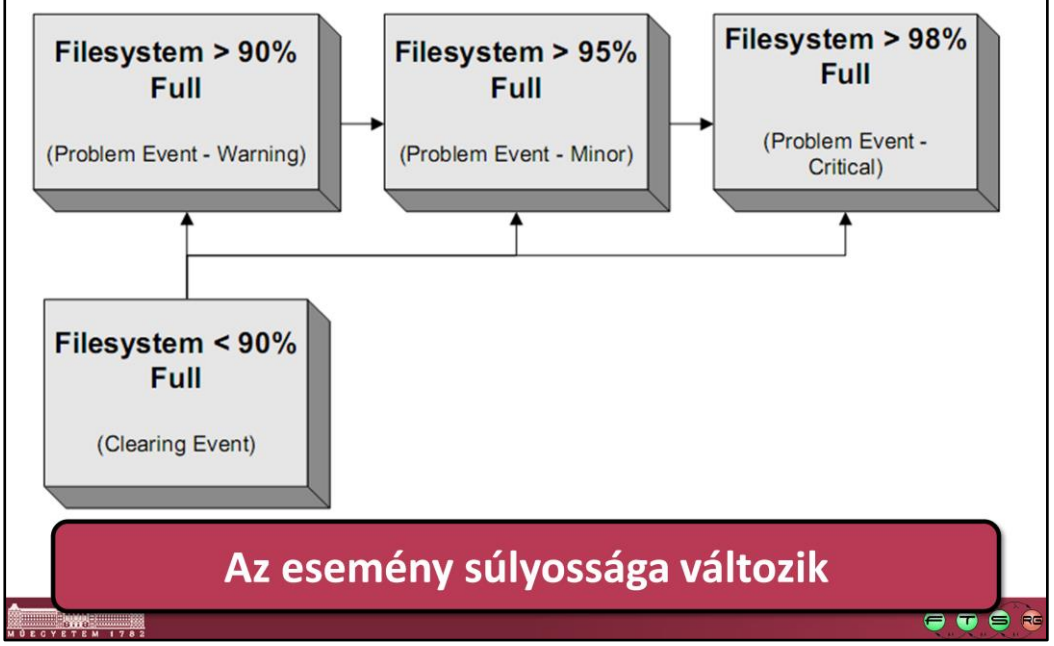


Ok: switch reboot
Megjegyzés: az email több szempontból sem tökéletes eszköz

Netcool/OMNIbus Event List



Korreláció: esemény-eszkaláció



Az esemény súlyossága változik

A feldolgozás jellemző lépései (folyt.)

- Esemény-eszkaláció
  - Kiválthatja időzítés és
  - a probléma üzleti hatása is.
- Események állapotváltásának szinkronizálása feldolgozók között
- Megfelelő személyzet értesítése (notification)
- Átvezetés a hibabélyeg-kezelő rendszerbe (trouble ticketing)

Célvezérelt eseménykezelés?

- Adott rengeteg eseményforrrás
  - Naplók, monitorozás, platform eseménykezelők, …
- Tfh. adott egy ese
  - Sok „enterprise” termék, de a FOSS is alternatíva
- Tfh. adott A Cél
  - Pl.: „proaktív hibahatás-elkerülés re
    infrastruktúrán”
- Források és feldolgozás konfiguráció-tervezése
  - Default + „mérnöki tapasztalat” + egyszerű intelligencia + folyamatos csiszolás
  - Modellvezérelt tervezés?

Honnan mi kell, milyen gyakran, …

Konfiguráció?

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