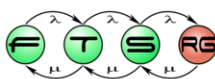


Eseménykezelés

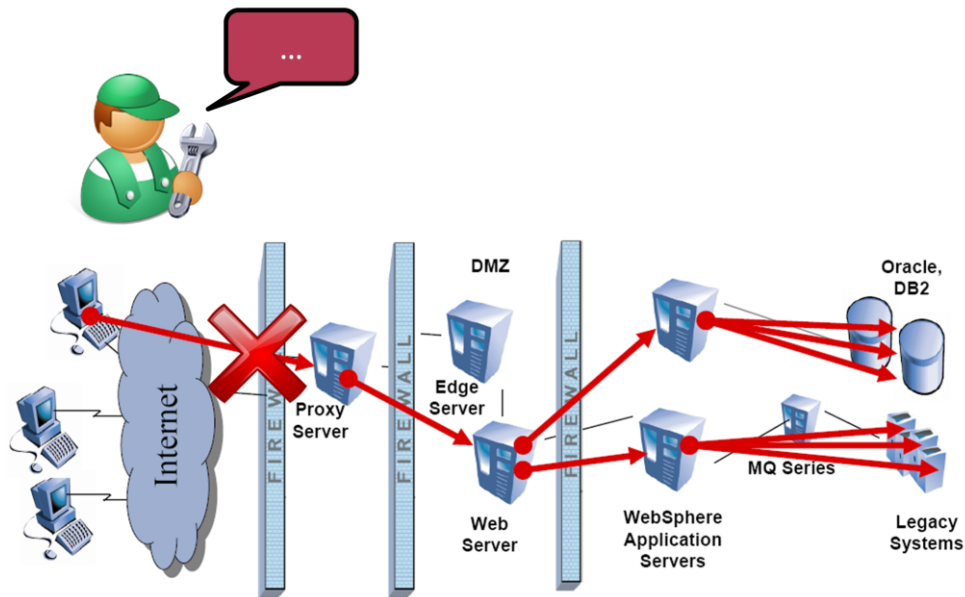
Kocsis Imre

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

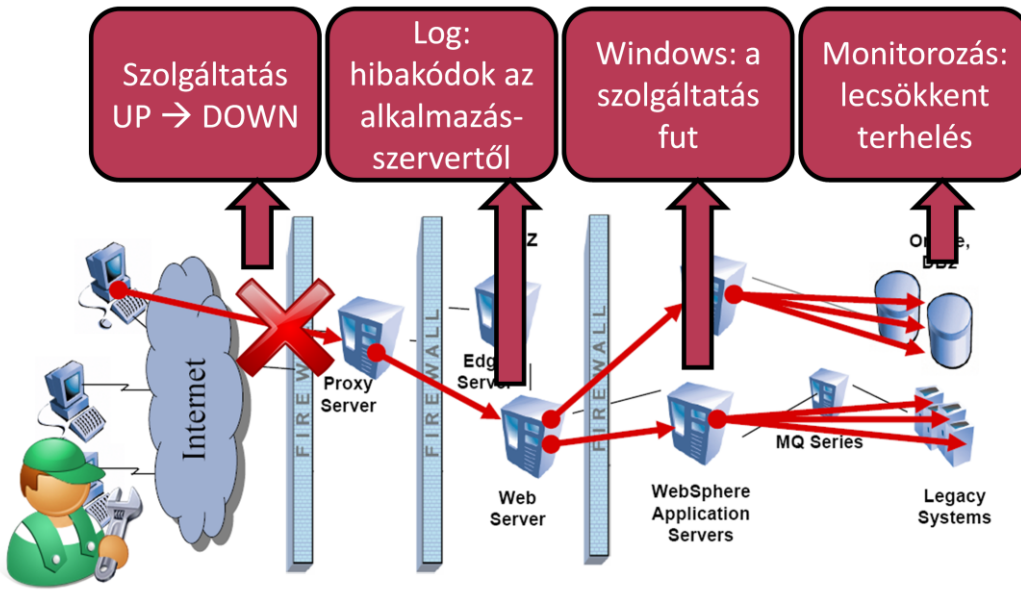


Utolsó módosítás: 2011.04.07.

Motiváció



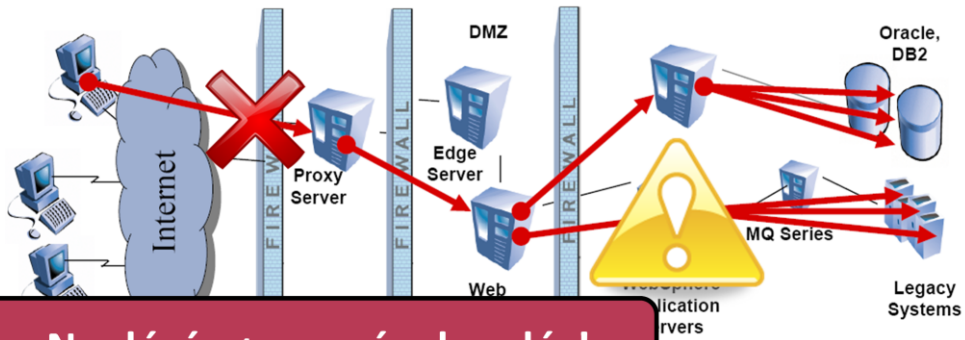
Motiváció



Motiváció



Az események széleskörű figyelése elengedhetetlen; igaz, sok egyidejű esemény intelligens feldolgozása nehéz.



Naplózás ≠ eseménykezelés!

Az „esemény” fogalma

- Az IT szolgáltatás- és rendszerfelügyeletben az **esemény** olyan **adat**, ami egy vagy több **erőforrásról**, illetve **szolgáltatásról** 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

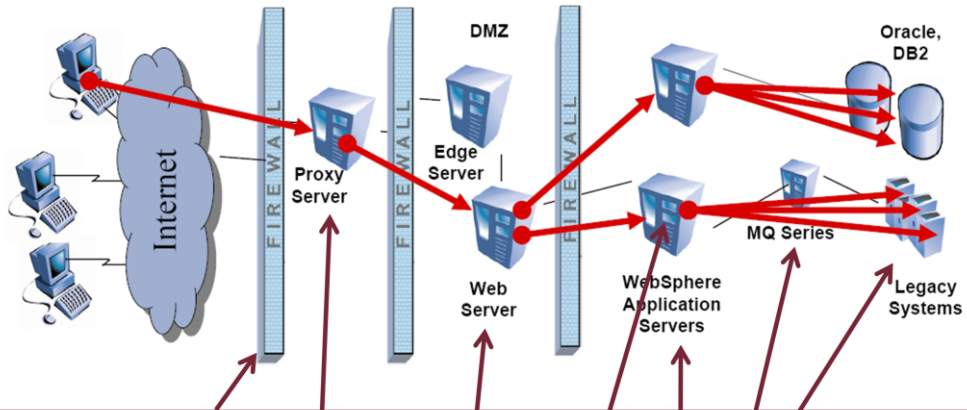
Jellemző események egy IT infrastruktúrában

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

- Service Level Agreement-ek eseményei
 - SLA megsértése (SLA breach)
 - SLA-sértés közeli állapotba kerülés
 - ...

A felsorolás nyilván folytatható. (Sokáig.)

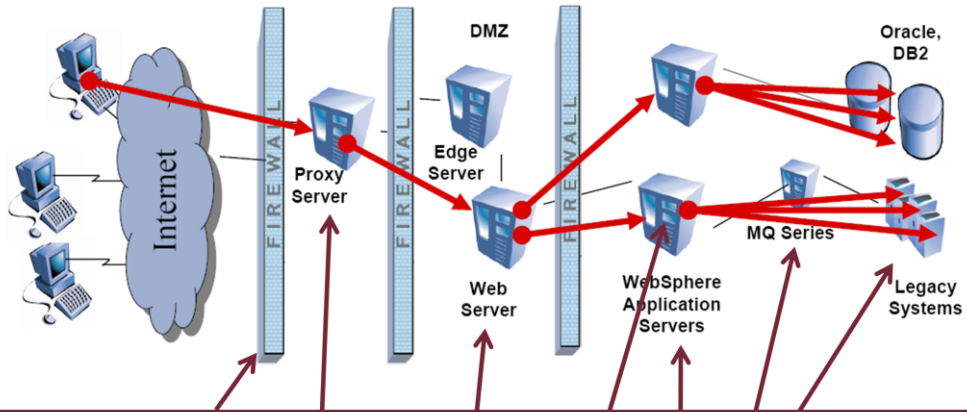
Események egy IT infrastruktúrában



Események

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

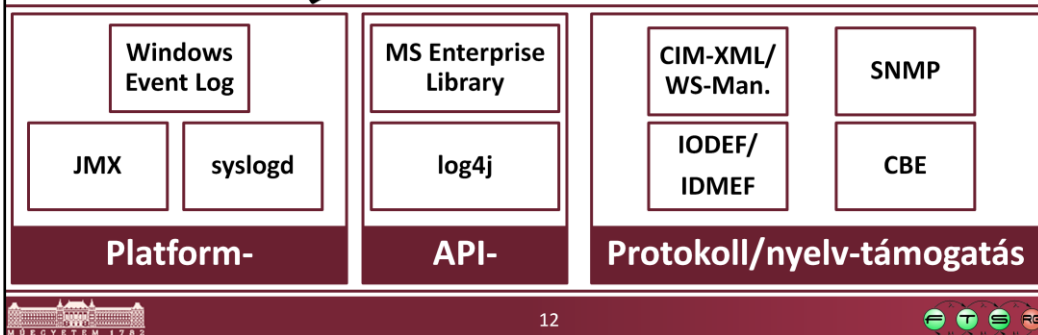
Események egy IT infrastruktúrában



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

Az „eseménykezelés” aspektusai

1. Valójában a határok nem ilyen élesek
2. Ezen a szinten: regisztrálás (osztályozással), továbbítás



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

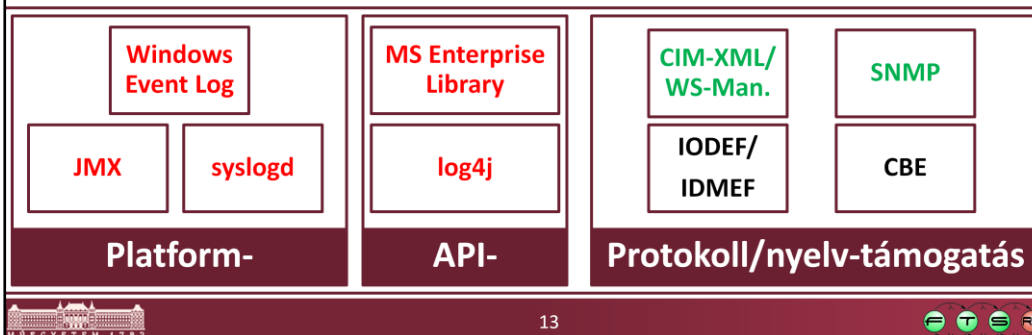
A Microsoft Enterprise Library („a set of tools and programming libraries for the Microsoft .NET Framework”) „Logging Application Block”-ja ad loggolást támogató API-t és mechanizmusokat; ez sokban hasonlít pl. a log4j-re a Java világból. Ezeket külön is fogjuk tárgyalni.

A már megismert protokollok mind támogatják események átvitelét (a saját adatmodelljük kontextusában értelmezve azokat); említést érdemelhet még pl. a „Common Base Event”

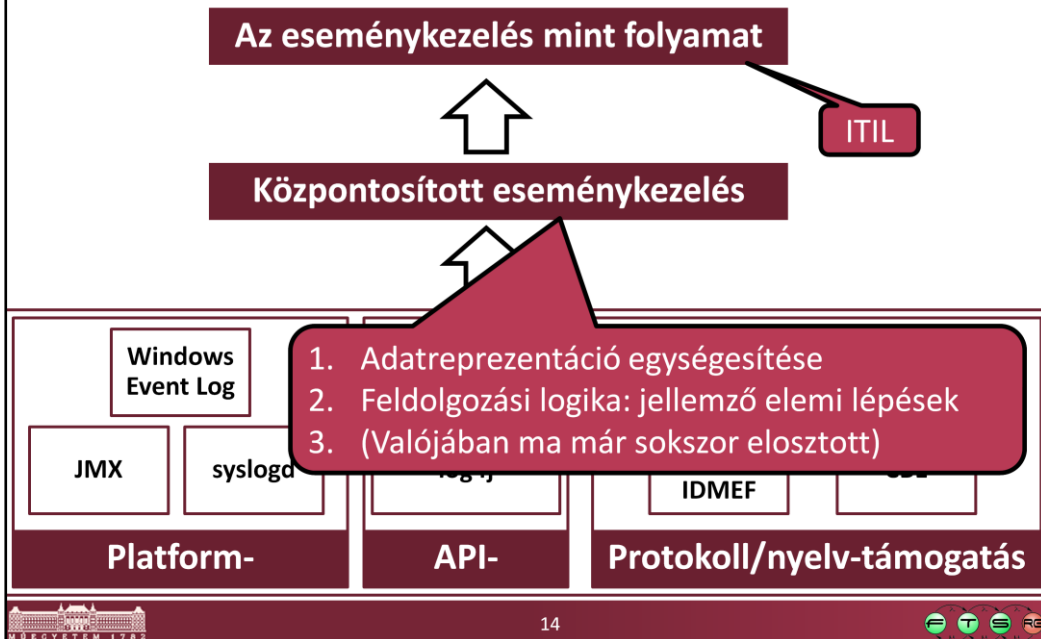
(<http://www.ibm.com/developerworks/library/specification/ws-cbe/>) leírónyelv és az Incident Object Description and Exchange Format (IODEF - <http://xml.coverpages.org/iodef.html>) / Intrusion Detection Message Exchange Format (IDMEF - <http://www.ietf.org/rfc/rfc4765.txt>).

Figyelem: a listák legjobb esetben is csak reprezentatívak, nem pedig teljesekek.

Az „eseménykezelés” aspektusai



Az „eseménykezelés” aspektusai



Az adatrepresentáció 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 Event Viewer

- Indítás, ismerkedés
- Néhány konkrét esemény
- Create Custom View
 - Mi ott az az XML fül?
 - Szűrés Xpath-szal



18



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

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
- 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

**További alapfogalmak:
következő előadás**



Esemény-továbbítás

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



„Nehézszűű” eseménykezeléshez azért több kell

syslogd

„syslogd”

- Történelmi okokból a de-facto szabvány naplókiszolgáló UNIX-okon és GNU/Linux-on
 - kernel üzeneteknek Linuxon (lehet) külön klogd
 - „Adatmodell” és protokoll: RFC 3164 (2001!)
- Démon, mely tud figyelni:
 - Unix domain socket-en (helyi IPC socket; /dev/log)
 - UDP porton (514-es port)
- Egy üzenet javasolt felépítése:

PRI HEADER MSG

„syslogd”

- Történelmi okokból a de-facto szabvány napló-kiszolgáló UNIX-okon és GNU/Linux-on
 - kernel üzeneteknek Linuxon (lehet) külön klogd
 - „Adatmodell” és 64 (2001!)
- D...
 - 8* „facility” + „severity”
 - Időbélyeg és hosznév
 - Program/folyamat neve és tartalom
- Egy üzenet javasolt felépítése:

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
# Don't log 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                                     *
```

```
#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                                     *
```



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 fut
- ...

**Viszont valamennyire
„közös nevező”**

**Egyébként: mi van a saját
naplót használó
alkalmazásokkal?**

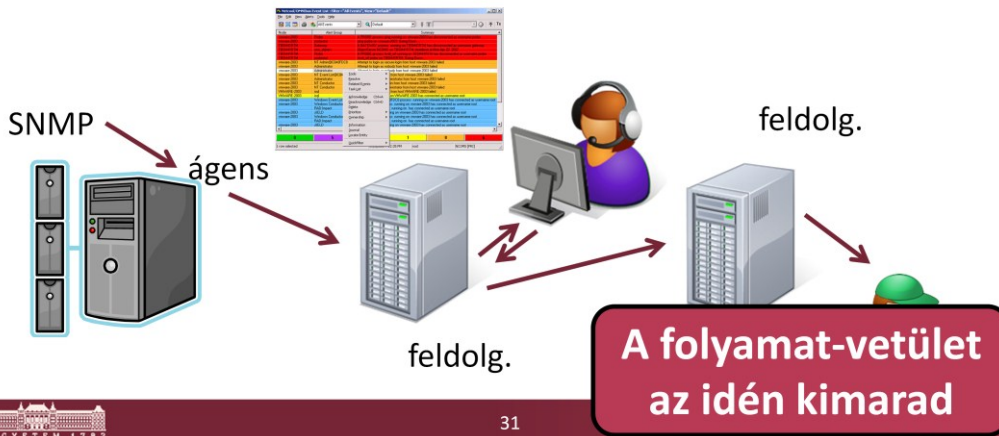
Felhasznált forrás: <https://unixlinux.tmit.bme.hu/Naplózás>



Eseménykezelés

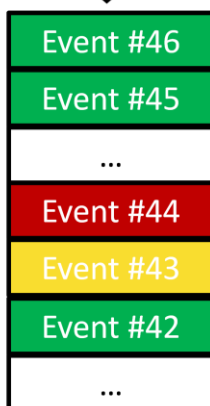
Esemény-feldolgozás

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



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):

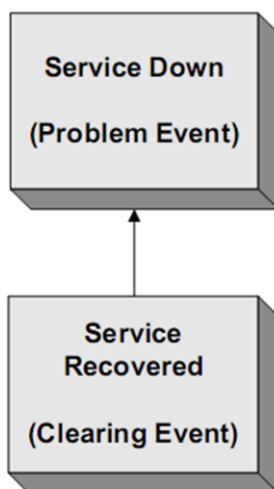
1.3.2 Filtering and forwarding

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.

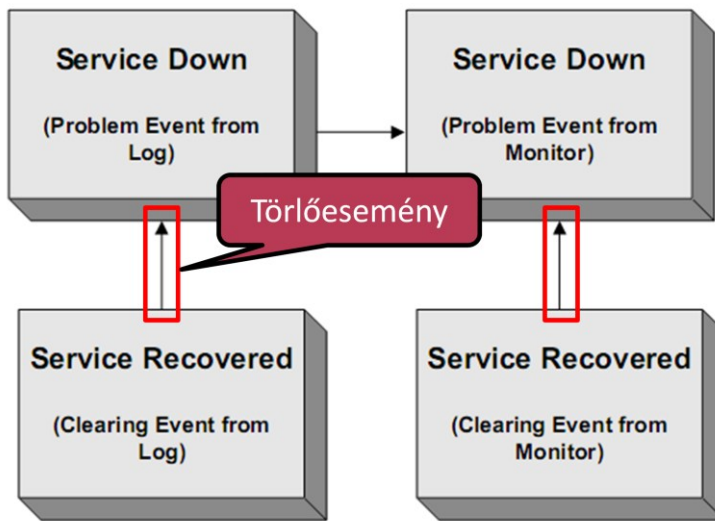
Korreláció: probléma- és törlőesemény



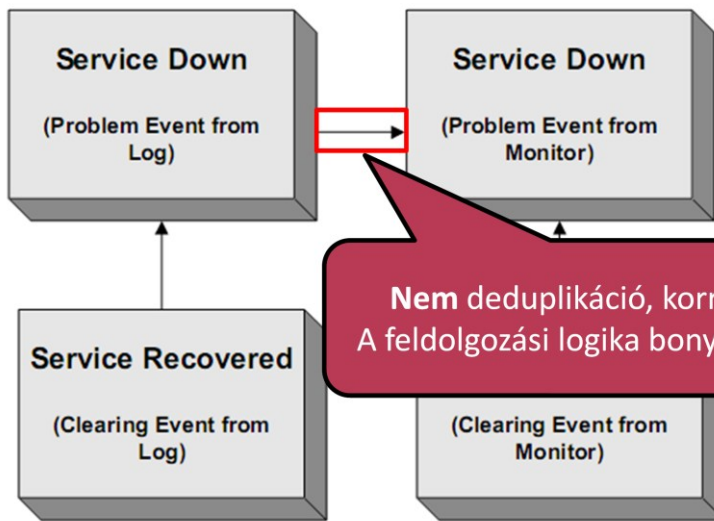
„Clearing event” beérkezésekor az eredeti „Problem event”-et általában *lezárjuk*; egyszerűbb esetben *töröljük* (bár ez sérthet auditálhatósági követelményeket).

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.

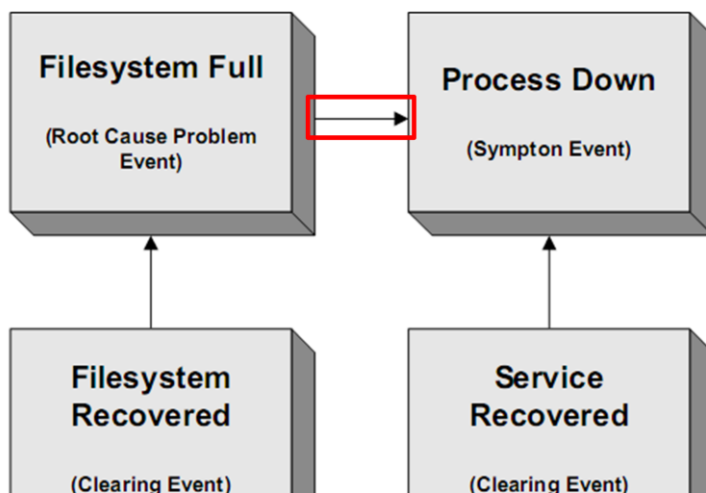
Törlőesemény-korreláció: bonyolultabb példa



Törlőesemény-korreláció: bonyolultabb példa



„Kiváltó ok” (root cause) korreláció



**Általában elnyomás (supression).
Legtöbbször topológia-alapú
(fizikai + telepítési + szolgáltatásfüggőségi)**

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”

Keresés: notifications (Ctrl+E)

Rendezési szempont: Dátum (Témák)

- Host UP alert for luthien!
nagios@celeborn.mit.bme.hu 2011.03...
- Host UP alert for beren!
nagios@celeborn.mit.bme.hu 2011.03...
- Host DOWN alert for salvador!
nagios@celeborn.mit.bme.hu 2011.03...
- Host UP alert for aragorn!
nagios@celeborn.mit.bme.hu 2011.03...
- Host DOWN alert for aragorn!
nagios@celeborn.mit.bme.hu 2011.03...
- Host DOWN alert for luthien!
nagios@celeborn.mit.bme.hu 2011.03...
- Host DOWN alert for melian!
nagios@celeborn.mit.bme.hu 2011.03...
- Host DOWN alert for miriel!
nagios@celeborn.mit.bme.hu 2011.03...
- Host DOWN alert for arwen!
nagios@celeborn.mit.bme.hu 2011.03...
- Host DOWN alert for ugluk!
nagios@celeborn.mit.bme.hu 2011.03...
- Host DOWN alert for beren!
nagios@celeborn.mit.bme.hu 2011.03...

Host DOWN alert for beren!

nagios@celeborn.mit.bme.hu

Küldve: P 2011.03.18. 16:06

Címzett: nagios@celeborn.mit.bme.hu

***** Nagios *****

Notification Type: PROBLEM
Host: beren
State: DOWN
Address: 152.66.252.233
Info: CRITICAL - Host Unreachable (152.66.252.233)

Date/Time: Fri Mar 18 16:06:25 CET 2011

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

Netcool/OMNibus Event List

Netcool/OMNibus Event List : Filter="All Events", View="Default"

File Edit View Alerts Tools Help

All Events Default

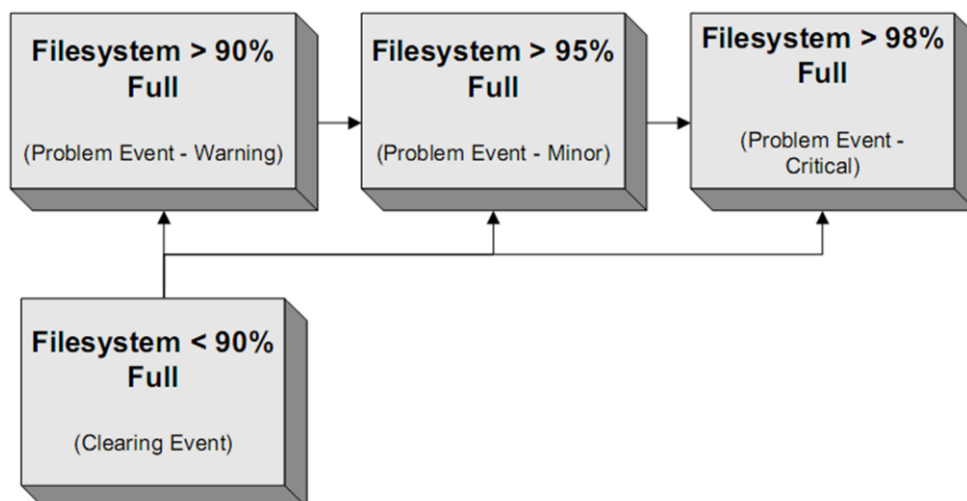
Node	Alert Group	Summary
vmware-2003	Probe	A PROBE process ping running on vmware-2003 has disconnected as username probe
vmware-2003	probestat	ping probe on vmware-2003: Going Down
TBSM41RTM	Gateway	A GATEWAY process running on TBSM41RTM has disconnected as username gateway
TBSM41RTM	nco_observ	ObjectServer NCOMS on TBSM41RTM shutdown at Mon Apr 23 2007
TBSM41RTM	Probe	A PROBE process tivoli_elf running on TBSM41RTM has disconnected as username probe
TBSM41RTM	probestat	tivoli_elf probe on TBSM41RTM: Going Down
vmware-2003	NT Admin@C0A8FDC8	Attempt to login as secure-login from host vmware-2003 failed
vmware-2003	Administrator	Attempt to login as nobodz from host vmware-2003 failed
vmware-2003	Administrator	Attempt to login as nobody from host vmware-2003 failed
vmware-2003	Administrator	Administrator from host vmware-2003 failed
vmware-2003	NT Conductor	in from host vmware-2003 failed
vmware-2003	NT Conductor	Administrator from host vmware-2003 failed
VMWARE-2003	isql	from host VMWARE-2003 failed
VMWARE-2003	isql	on VMWARE-2003 has connected as username root
vmware-2003	Windows Event List	BDFC8 process running on vmware-2003 has connected as username root
vmware-2003	Windows Conductor	ss running on vmware-2003 has connected as username root
vmware-2003	RAD:Impact	running on has connected as username root
vmware-2003	JJELD	ing on vmware-2003 has connected as username root
vmware-2003	Windows Conductor	ss running on vmware-2003 has connected as username root
vmware-2003	RAD:Impact	running on has connected as username root
vmware-2003	JJELD	ing on vmware-2003 has connected as username root

0 5 1 8 6

1 row selected 2:35 PM root NCOMS [PRI]



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 eseményforrás
 - Naplók, monitorozás, platform eseménykezelők, ...
- Tfh. adott egy eseményfeldolgozó 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
 - Default + „mérnöki tapasztalat” + egyszerű intelligencia + folyamatos csiszolás
 - Modellvezérelt tervezés?

Linkek – Windows eseménykezelés

- Rövid áttekintés a Windows eseménykezelésről
 - [http://msdn.microsoft.com/en-us/library/aa382610\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa382610(VS.85).aspx)
 - http://en.wikipedia.org/wiki/Event_Viewér
- 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>



[http://msdn.microsoft.com/en-us/library/aa382610\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa382610(VS.85).aspx)

http://en.wikipedia.org/wiki/Event_Viewér

<http://blogs.technet.com/otto/archive/2008/07/08/quick-and-dirty-enterprise-eventing-for-windows.aspx>

<http://msdn.microsoft.com/en-us/library/bb756956.aspx>

<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>



<http://en.wikipedia.org/wiki/Syslog>

<http://www.ietf.org/rfc/rfc3164>

<http://www.sans.org/rr/whitepapers/logging/1168.php>

<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



<http://www.redbooks.ibm.com/abstracts/sg246094.html?Open>

http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.netcool_OMNIbus.doc_7.2.1/welcome.htm