

Logelemzés virtualizációs környezetben

Virtualizációs Nap 2011 - 2011. november 25.

Vámos Balázs, LOGalyze

Magamról

- A LOGalyze projekt fejlesztési vezetője
 - Stratégiai és koncepcionális tervezés
 - Projekt vezetés
 - Fejlesztés irányítása
- Fejlesztő → Üzemeltető → CISA
- Loggyűjtéssel és elemzéssel foglalkozó mérnök
 - Pre-sales
 - Tervezés, bevezetés

Miről is lesz szó?

- Interaktív beszélgetés a logelemzésről, fókuszba helyezve a virtualizációs környezetek használata során felmerülő új kihívásokat
- Bátran szóljanak közbe! Nem felejttem el hol tartottam :-)
- Általam használt fogalmak (log/napló, vm, host/guest, elemzés, korreláció)

Általában a naplóelemzésről

- Különböző szemléletek, mindenki másra kíváncsi
 - A Rendszergazda üzemeltet
 - Keresés (grep), korrelációs listázás (grep | grep | grep), statisztikák, riasztás
 - A biztonsági főnök “kötözködik”
 - Végtelen bonyolultságú korrelációs szabályok
 - Az auditor ellenőríz
 - Automatizált jelentések

Korrelációs elemzés a LOGalyze-ban

- Definíció alapú működés: Event Definitions
 - Egyszerű szabály
 - Korrelációs szabályok
 - Threshold
 - 2 thresholds
 - Rule group
 - Állapot kezelés (Context)
 - Akció lista

Logelemzés virtualizációs környezetben

- Vannak-e újdonságok, amikkel eddig nem találkoztunk? *Ez fáj a legjobban.*
- Mi az, ami változik az új környezettel? *Csak kicsit fáj.*
- Mi marad ugyanaz? *Megkönnyebbülés.*
- Van-e olyan körülmény, ami eltűnik a virtualizáció bevezetésével? *Heuréka!!!!*

Mi marad?

- Az infrastruktúra többi része mindenképpen megmarad (hálózati elemek, határvédelem, SAN, stb.)
- Ugyanazok az operációs rendszerek
- A hangsúly továbbra is a változáskezelésen van
 - Rendszerek jönnek, mennek, módosulnak
 - Az alapvető feladat a rendszerek használata marad

Újdonságok a virtualizációval

- Új logforrások mindenképpen megjelennek
- Az új eszközök új típusú fenyegetettségeket hoznak magukkal
- Az új fenyegetettségek új kihívásokat állítanak a logelemzés elé
 - A rendszereink gyakrabban és gyorsabban változnak
 - Új VM-ek jönnek létre, mozognak, tűnnek el, ráadásul **fizikai jelenlét ehhez már nem szükséges**

Mi változik még?

- A legfontosabb új szereplő az infrastruktúrában a **Host szerver**
 - Szigorúbb felügyelet
 - Szigorúbb biztonsági ellenőrzés
- Új management eszközök jelennek meg (management console, management szerver) ezek logjai hordozhatják a legfontosabb információt

Előnyök, hátrányok

- Új VM telepítésekor még könnyebb a megkövetelt biztonsági paraméterek, szoftverek beállítása (template)
- Nincs szükség a meglévő egyéb eszközeink cseréjére, használhatjuk a meglévő okosságokat az elemzéskor

Előnyök, hátrányok

- Mindenképpen megjelennek új logok, amik közt sok a kritikus. Ezeket gyűjteni, elemezni kell.
- A logmennyiség szinte biztosan nő :-)
- Nem csak az üzletet kiszolgáló szerverekkel, hanem az azokat kiszolgáló szerverekkel is foglalkozni kell
- Előfordulhat, hogy olyan eszközöket is a felügyelet alá kell vonni, amikről nem is tudunk, olyan logelemzés kell, ami ezeket automatikusan felismeri

Megközelítési módok

- Biztonság alapú
 - Hozzáférésekre összpontosít (account activity) a host és a guest gépeken egyaránt
 - Biztonsággal kapcsolatos hibák felismerése és elemzése a cél
 - Anomáliák kiszűrése fontos, de nagyon egyediek az igények (a világ összes számítási kapacitása is kevés lenne)

Megközelítési módok

- Üzemeltetés oldaláról
 - Működéssel kapcsolatos hibák és figyelmeztetések
 - Működési paraméterek (health) figyelése
 - Nagios vs. LOGalyze
 - Virtualizáció egyik fő célcsoportja a cluster rendszerek, összetartozó logok több helyen keletkeznek, ezeket kezelni kell, nincs elemzés korreláció nélkül

Megközelítési módok

- Megfelelőségi (audit szemléletű)
 - Szabványok, előírások, ajánlások szerinti megfelelés ellenőrzése
 - Automatizált jelentések nagyon fontosak
 - Valós idejű riasztásoknak nincs különösebb jelentősége

Kilátások

- A naplóelemzés fontossága folyamatosan nő
- Gyűjteni már nagyon jól tudunk, igazán elemezni kevésbé
- Igény van, de konkrét elképzelések sajnos ritkán vannak, ha vannak, inkább üzemeltetési oldalról
- Fontos cél az integráció egyéb eszközökkel, majd a kapcsolatok felismerése

A fejlődés kézzelfogható jelei

- VMware ESXi 3.5, 4 host log fájlok
 - `/var/log/messages`: Core VMkernel logs, including device discovery, storage and networking device and driver events, virtual machine startup, and a merged copy of the `hostd` and `vpixd` management service logs.
 - `/var/log/vmware/hostd.log`: Host management service logs, including virtual machine and host Tasks and Events, communication with the vSphere Client and vCenter Server `vpixd` agent, and SDK connections.
 - `/var/log/sysboot.log`: Early VMkernel startup, module loading, and host initialization.

A fejlődés kézzelfogható jelei

- vmware ESXi 5.0 host log fájlok
 - /var/log/auth.log: ESXi Shell authentication success and failure.
 - /var/log/dhclient.log: DHCP client service, including discovery, address lease requests and renewals.
 - /var/log/esxupdate.log: ESXi patch and update installation logs.
 - /var/log/hostd.log: Host management service logs, including virtual machine and host Task and Events, communication with the vSphere Client and vCenter Server vpxa agent, and SDK connections.
 - /var/log/shell.log: ESXi Shell usage logs, including enable/disable and every command entered.
 - /var/log/sysboot.log: Early VMkernel startup and module loading.
 - /var/log/syslog.log: Management service initialization, watchdogs, scheduled tasks and DCUI use.
 - /var/log/usb.log: USB device arbitration events, such as discovery and pass-through to virtual machines.
 - /var/log/vob.log: VMkernel Observation events, similar to vob.component.event.
 - /var/log/vmkernel.log: Core VMkernel logs, including device discovery, storage and networking device and driver events, and virtual machine startup.
 - /var/log/vmkwarning.log: A summary of Warning and Alert log messages excerpted from the VMkernel logs.
 - /var/log/vmksummary.log: A summary of ESXi host startup and shutdown, and an hourly heartbeat with uptime, number of virtual machines running, and service resource consumption.

Összefoglalás

- Nem egy teljesen új környezettel van dolgunk, csak a meglévőknek új elemei vannak
- Új logok → Új információk → Új kihívások
- Meg kell tanulnunk a VM platform új eseményeit
- Nekünk kell alkalmazkodnunk az új virtualizációs rendszerekhez

Köszönöm a figyelmet!

www.logalyze.com