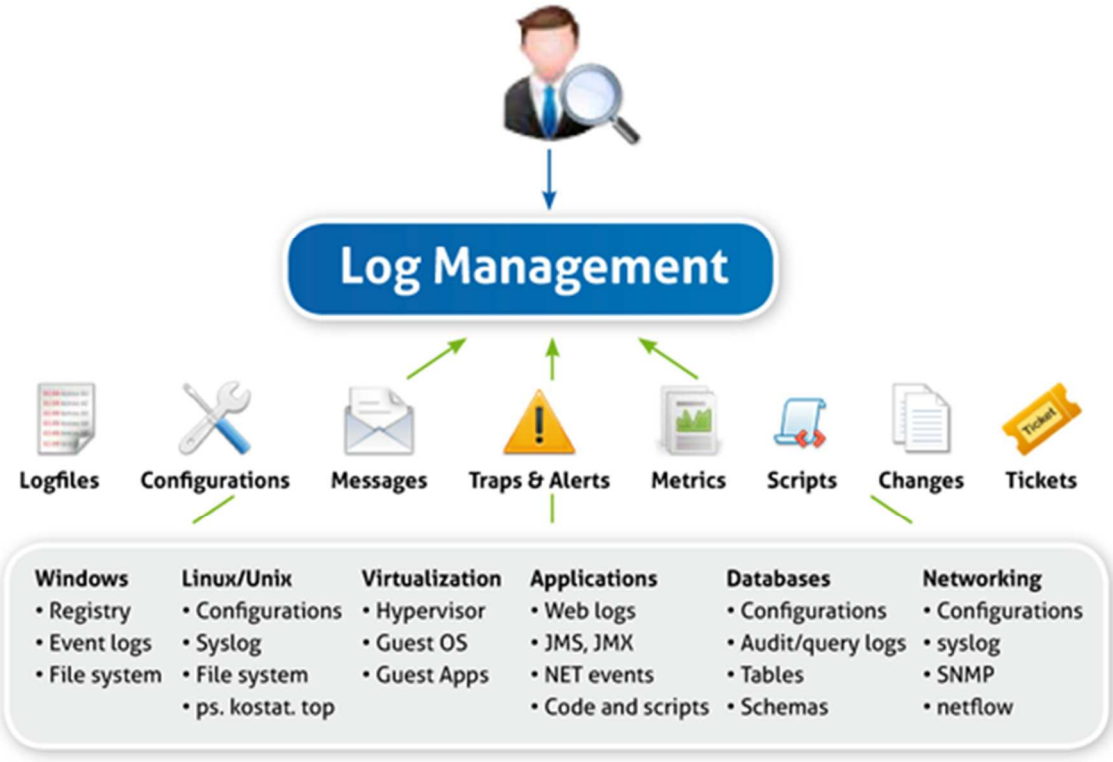
Systematický log management

Na každou společnost má dopad rostoucí komplexita ICT. Současná datová centra se rychle vyvíjejí a tak se stávají velmi komplexní vrstevnatou skupinou technologií tvořících vzájemně propojená datová a systémová úložiště pracující v prostředí bez zřetelných hranic. Když se objeví nějaký problém, nalezení skutečné příčiny je velmi obtížné stejně jako získání přehledu napříč infrastrukturou tak, abychom mohli aktivně identifikovat výpadek a zabránit mu. Je stále obtížnější zajišťovat:

- rychlou analýzu provozních problémů
- nízkou dobu neplánovaných výpadků
- co nejpřesnější plánování rozvoje kapacit a výkonnosti ICT zdrojů

Typické nástroje pro správu a monitoring ICT infrastruktury nejsou schopny držet krok s de facto konstantní změnou, která se děje v datových centrech a celé infrastruktuře. Tyto systémy jsou nepružné, drahé a nejsou navrženy pro komplexitu současných systémů. Kromě toho jejich přístup k monitoringu je často založen na filtraci a sumarizaci. Když se objeví provozní problém, nejsou obvykle schopny jednoduše metodou drill down analyzovat skutečnou příčinu problému. Obtíže v získání přístupu k datům se tak přidávají k řešení problému samotného.



Schopnost propojit různé případy výkonnostních problémů a výpadků je extrémně důležitá, neboť tradiční nástroje jsou orientovány na technologická sila a nemohou přistupovat a analyzovat všechny relevantní události napříč ICT prostředím.

Proaktivní monitoring

Moderní řešení jsou souborem integrovaných a škálovatelných nástrojů pro sběr, indexaci a tvorbu vazeb v systémových datech generovaných on-line z jakéhokoliv systémového zdroje, lokality a v libovolném formátu. Můžeme do nich zahrnout všechny zdroje ICT infrastruktury – komunikační infrastrukturu, servery, databáze, aplikace a přitom ke každé z těchto oblastí můžeme přistoupit ještě detailněji – HW, operační systém, apod.

Použitím takovýchto řešení dosáhneme provozního přehledu v každé vrstvě používaného ICT prostředí. Jsme tak schopni přeměnit obrovské objemy systémových dat na integrované a využitelné informace dostupné v jednom centralizovaném místě.

Redukováním střední doby vyšetření incidentu (MTTI - Mean Time To Investigate) a tím střední doby opravy (MTTR – Mean Time To Repair) jsme schopni udržovat kritické aplikace v chodu a nalézat a odstraňovat problémy rychleji než kdykoli předtím.

Monitoring a analýza změn a chybových stavů systémových zdrojů

Funkcionalitu monitoringu a rychlé analýzy změn a chybových stavů systémových zdrojů jsme schopni bezezbytku realizovat pomocí nástrojů pro log management.

Systémy log managementu jsou vysoce škálovatelné nástroje pro sběr, indexaci a tvorbu vazeb v systémových datech generovaných on-line z jakéhokoliv systémového zdroje, lokality a v libovolném formátu. Do log managementu můžeme zahrnout všechny zdroje ICT infrastruktury – komunikační infrastrukturu, servery, databáze, aplikace a přitom ke každé z těchto oblasti můžeme přistoupit ještě detailněji – HW, operační systém.

Log management nám umožní prověřit data a korelovat problémy v souvislosti s dostupností služeb napříč všemi úrovněmi využívané informační architektury. Můžeme monitorovat změny, které mohou způsobit provozní problémy. Lze kombinovat analýzu dat v reálném čase s korelacemi v TB historických dat k detekování vzorků, které mohou pomoci predikovat problémy, a tak zabraňovat výpadkům.

Přínosy využití systému pro log management

- výrazné zvýšení schopnosti rychlé analýzy provozního problému (zkrácení MTTI)
- snížení celkové doby neplánovaných výpadků (zkrácení MTTR)
- rozšíření možnosti přesnějšího plánování výkonnosti a kapacity zdrojů (historická data)
- prokazatelné zvýšení dostupnosti ICT služeb
- získání podkladů pro relevantní SLA
- specialisté budou osvobozeni od rutinních činností a mohou věnovat více času podpoře uživatelů
- řešení vyhovuje systematickému přístupu dle standardů (FCAPS/ITIL)
- ekonomickou výhodou je relativně krátká doba implementace a nízké finanční náklady