ICZ Log Manager 2

Security information and event management

VIETE, KDE MÁTE SVOJE LOGY? VIETE V NICH RÝCHLO NÁJSŤ POTREBNÉ INFORMÁCIE? VIETE, KTO VÁM ZAMKOL KONTO? KTO VČERA VYUŽÍVAL URČITÚ SLUŽBU? AKO ČASTO SA DEJÚ NIEKTORÉ UDALOSTI? ODPOVEDE NA TIETO A NA PODOBNÉ OTÁZKY NÁJDETE POMOCOU NÁŠHO RIEŠENIA.

Intenzívny rozvoj informačných technológií v poslednom čase so sebou prináša aj značný nárast množstva zaznamenávaných činností v podobe udalostí. Záznamy mnohých činností síce bývajú niekde ukladané, avšak sú ťažko dostupné a z prevádzkových dôvodov sa ukladajú iba po obmedzený čas. Na vine je väčšinou zložitosť a prácnosť analýzy veľkého objemu údajov alebo nemožnosť ukladať jeho stále rastúce množstvo. Preto treba včas určiť stratégiu, akým spôsobom sa bude s udalosťami nakladať, ako sa budú zbierať, normalizovať, ukladať, archivovať a vyhodnocovať.

**VLASTNOSTI A VÝHODY**

` **Zber systémových aj aplikačných udalostí z Windowsu, Linuxu**

**a VMware**

` **Príjem udalostí protokolom Syslog**

` **Normalizácia formátu udalostí umožňujúca jednoduché vyhodnotenie udalostí rovnakého typu naprieč rôznymi typmi zariadení**

` **Uloženie udalostí do NOSQL databázy s fulltextovým vyhľadávaním**

` **Moderné webové rozhranie pre vyhľadávanie a vizualizáciu udalostí s dashboardmi pre opakované činnosti**

` **Archivácia udalostí v tvare JSON na dlhodobé uloženie nezávislé od nástroja na ich spracovanie**

# [ ICZ LOG MANAGER ]

Komplexný a veľmi efektívny spôsob práce s udalosťami predstavuje aplikácia ICZ Log Manager. Jej základom je NOSQL databáza s podporou pre fulltextové vyhľadávanie. Uložené udalosti sú k dispozícii prostredníctvom moderného webového rozhrania s podporou ad-hoc prehľadávania a dashboardy pre opakované činnosti. Dashboardy využívajú široké palety vizualizácií, najmä rôzne typy grafov a zobrazenia geografických informácií na mape.

Pri zbere udalostí je vykonávaná ich normalizácia do jednotného slovníka v  tvare JSON, čo umožňuje zjednotiť význam jednotlivých polí udalostí nezávisle od ich pôvodu a zabezpečiť tak ucelené vyhodnotenie udalostí bez ohľadu na typ zariadenia. Udalosti sú ďalej obohatené o kategorizujúce metaúdaje a doplnené chýbajúce DNS názvy a IP adresy.

# [ PRÁVNE POŽIADAVKY ]

Veľa zákonných noriem (zákon o kybernetickej bezpečnosti, zákon o ochrane osobných údajov, GDPR) požaduje, aby organizácie vykonávali zber, archiváciu a následné vyhodnotenie udalostí a archivovali zozbierané udalosti. ICZ Log Manager je navrhnutý tak, aby vyhovel týmto požiadavkám platným v Českej republike.

# [ ZBER UDALOSTÍ ]

ICZ Log Manager umožňuje príjem udalostí protokolom Syslog a obsahuje agenty pre operačné systémy Windows, Linux a VMware vSphere a vCenter umožňujúce zber systémových a aplikačných logov v textových súboroch. Riešenie je možné doplniť o agenty na zber logov uložených v SQL databázach.

Na nasadenie v rozsiahlych sieťach je možné využiť ICZ Log Collector, ktorý prijíma udalosti v lokalite a odosiela ich do centrálneho ICZ Log Managera. V prípade problémov s komunikáciou ukladá udalosti na disk a odosiela ich po opätovnom nadviazaní spojenia.

# [ NORMALIZÁCIA UDALOSTÍ ]

ICZ Log Manager vykonáva normalizáciu udalostí do jednotného slovníka so základným členením na:

` Metaúdaje o udalosti.

` Informácie o zariadení, ktoré udalosť vytvorilo.

` Informácie o subjekte, ktorý zapríčinil vznik udalosti.

` Informácie o objekte, ktorý bol udalosťou ovplyvnený.

**[ ICZ Log Manager 2 ]**

# [ OBOHATENIE UDALOSTÍ ]

Udalosti sú ďalej obohatené o nasledujúce metaúdaje a informácie:

` **Kategórizácia** umožňujúca zaradenie udalostí do oblasti (sieť, virtualizácia, počítač, aplikácia…), priradenie jednotného typu akcie (prihlásenie, prístup, modifikácia…), ich výsledku (úspech, odoprené, chyba…) a dôležitosť (informácia, varovanie, chyba…).

` IP adresy a DNS názvy – sú doplnené, ak jedna z nich chýba, DNS názvy sú doplnené o doménu.

# [ ARCHIVÁCIA LOGOV ]

` Udalosti v tvare JSON sú archivované do komprimovaných textových súborov, ktoré je možné ďalej spracovať podľa požiadaviek zákazníka.

# [ ULOŽENIE UDALOSTÍ DO DATABÁZY ]

` Udalosti v tvare JSON sú uložené po stanovený čas do NOSQL databázy a potom automaticky zmazané. V prípade potreby je možné vložiť staršie udalosti z archívu do databázy.

# [ VYHODNOTENIE UDALOSTÍ ]

` Webové rozhranie umožňuje vykonávať ad-hoc vyhodnotenie udalostí a vytvárať dashboardy pre pravidelne opakované činnosti. ICZ Log Manager obsahuje pripravený súbor vizualizácií a dashboardov, používatelia si potom môžu vytvárať svoje vlastné.

# [ MODULÁRNE RIEŠENIE ]

` ICZ Log Manager je modulárnym systémom, ktorý je možné prispôsobiť potrebám zákazníka od riešenia s jedným serverom pre jednu lokalitu po riešenie pre rozsiahle siete využívajúce klaster serverov pre škálovanie výkonu a/alebo kapacity a zber udalostí vo veľkom množstve lokalít.



**OBCHODNÝ KONTAKT**

**S.ICZ a. s.** Na hřebenech II 1718/10 140 00 Praha 4

**TEL.:** +420 222 271 111

**FAX:** +420 222 271 112

**E-MAIL:** marketing@i.cz