ICZ Log Manager 2

SECURITY INFORMATION AND EVENT MANAGEMENT

VÍTE, KDE MÁTE SVÉ LOGY? UMÍTE V NICH RYCHLE NAJÍT POTŘEBNÉ INFORMACE? VÍTE, KDO VÁM ZAMKL ÚČET? KDO VČERA VYUŽÍVAL URČITOU SLUŽBU? JAK ČASTO SE DĚJÍ NĚKTERÉ UDÁLOSTI? ODPOVĚDI NA TYTO A NA PODOBNÉ OTÁZKY NAJDETE POMOCÍ NAŠEHO ŘEŠENÍ.

Intenzivní rozvoj informačních technologií v poslední době s sebou přináší i značný nárůst množství zaznamenávaných činností v podobě událostí. Záznamy mnohých činností sice bývají někde ukládány, avšak jsou obtížně dostupné a z provozních důvodů jsou ukládány pouze po omezenou dobu. Na vině je většinou složitost a pracnost analýzy velkého objemu dat nebo nemožnost ukládat jeho stále rostoucí množství. Proto je třeba včas určit strategii, jakým způsobem se bude s událostmi nakládat, jak se budou sbírat, normalizovat, ukládat, archivovat a vyhodnocovat.

VLASTNOSTI A VÝHODY

- **Sběr systémových i aplikačních událostí z Windows, Linuxu a VMware**
- **Příjem událostí protokolem Syslog**
- **Normalizace formátu událostí umožňující snadné vyhodnocení událostí stejného typu napříč různými typy zařízení**
- **Uložení událostí do NoSQL databáze s fultextovým vyhledáváním**
- **Moderní webové rozhraní pro vyhledávání a vizualizaci událostí s dashboardy pro opakované činnosti**
- **Archivace událostí v JSON tvaru pro dlouhodobé uložení nezávislé na nástroji pro jejich zpracování**

[ICZ LOG MANAGER]

Komplexní a vysoce efektivní způsob práce s událostmi představuje aplikace ICZ Log Manager. Jejím základem je NoSQL databáze s podporou pro fulltextové vyhledávání. Uložené události jsou k dispozici prostřednictvím moderního webového rozhraní s podporou ad-hoc prohledávání a dashboardy pro opakované činnosti. Dashboardy využívají široké palety vizualizací, zejména různé typy grafů a zobrazení geografických informací na mapě.

Při sběru událostí je prováděna jejich normalizace do jednotného slovníku v JSON tvaru, což umožňuje sjednotit význam jednotlivých polí událostí nezávisle na jejich původu a zabezpečit tak ucelené vyhodnocení událostí bez ohledu na typ zařízení. Události jsou dále obohaceny o kategorizující metadata a doplněny chybějící DNS jména a IP adresy.

[PRÁVNÍ POŽADAVKY]

Řada zákonných norem (zákon o kybernetické bezpečnosti, zákon o ochraně osobních údajů, GDPR) požaduje, aby organizace prováděly sběr, archivaci a následné vyhodnocení událostí a archivovaly sebrané události. ICZ Log Manager je navržen tak, aby vyhověl těmto požadavkům platným v České republice.

[SBĚR UDÁLOSTÍ]

ICZ Log Manager umožňující také příjem událostí protokolem Syslog a obsahuje agenty pro operační systémy Windows, Linux a virtualizační formu VMware vSphere. Umožňuje také sběr systémových a aplikačních logů v textových souborech. Řešení je možné doplnit o agenty pro sběr logů uložených v SQL databázích.

Pro nasazení v rozsáhlých sítích je možné využít ICZ Log Collector, který přijímá události v lokalitě a odesílá je do centrálního ICZ Log Manageru. V případě problémů s komunikací ukládá události na disk a odesílá je po opětovném navázání spojení.

[NORMALIZACE UDÁLOSTÍ]

ICZ Log Manager provádí normalizaci událostí do jednotného slovníku se základním členěním na:

- Metadata o události.
- Informace o zařízení, které událost vytvořilo.
- Informace o subjektu, který zapříčinil vznik události.
- Informace o objektu, který byl událostí ovlivněn.

[OBOHACENÍ UDÁLOSTÍ]

Události jsou dále obohaceny o následující metadata a informace:

- **Kategorizace** umožňující zařazení událostí do oblasti (síť, virtualizace, počítač, aplikace...), přiřazení jednotného typu akce (přihlášení, přístup, modifikace...), jejich výsledku (úspěch, odepřeno, chyba...) a důležitost (informace, varování, chyba...).
- IP adresy a DNS jména - jsou doplněny, pokud jedna z těchto informací chybí. DNS jména jsou doplněna o doménu FQDN.

[ARCHIVACE LOGŮ]

- Události v JSON tvaru jsou archivovány do komprimovaných textových souborů, které je možné dále zpracovat podle požadavků zákazníka.

[ULOŽENÍ UDÁLOSTÍ DO DATABÁZE]

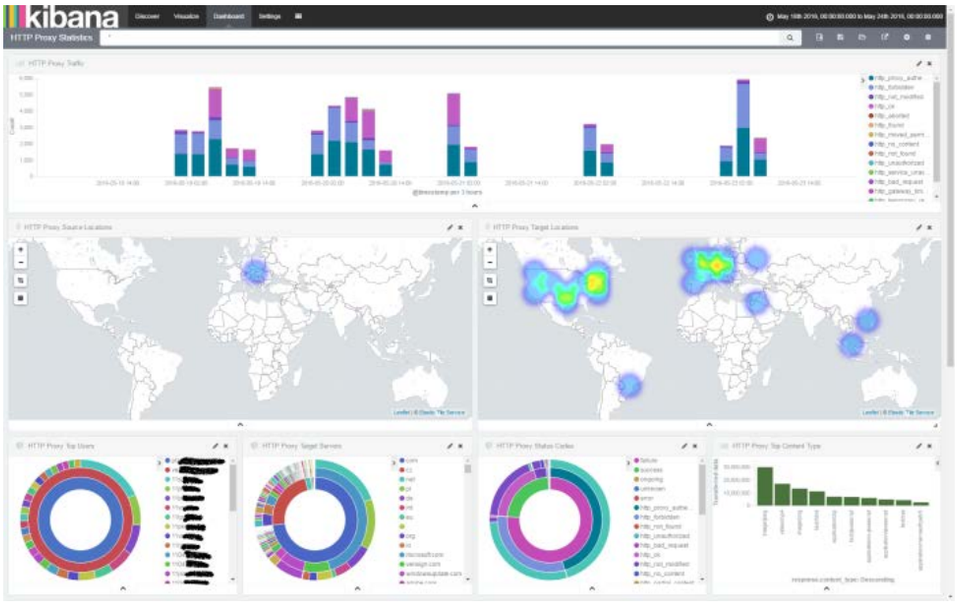
- Události v JSON tvaru jsou uloženy po stanovenou dobu do NoSQL databáze a poté automaticky smazány. V případě potřeby je možné vložit starší události z archivu do databáze.

[VYHODNOCENÍ UDÁLOSTÍ]

- Webové rozhraní umožňuje provádět ad-hoc vyhodnocení událostí a vytvářet dashboardy pro pravidelně opakované činnosti. ICZ Log Manager obsahuje připravenou sadu vizualizací a dashboardů, uživatelé si pak mohou vytvářet své vlastní.

[MODULÁRNÍ ŘEŠENÍ]

- ICZ Log Manager je modulární systémem, který je možné přizpůsobit potřebám zákazníka od řešení s jedním serverem pro jednu lokalitu po řešení pro rozsáhlé sítě využívající cluster serverů pro škálování výkonu a/nebo kapacity a sbírá události ve velkém množství lokalit.



OBCHODNÍ 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