

LOGmanager

- > Central Log Repository
- > Affordable SIEM



HELP TO RESOLVE
CRITICAL IT INCIDENT

» Případová studie - Krajská Nemocnice Jihlava

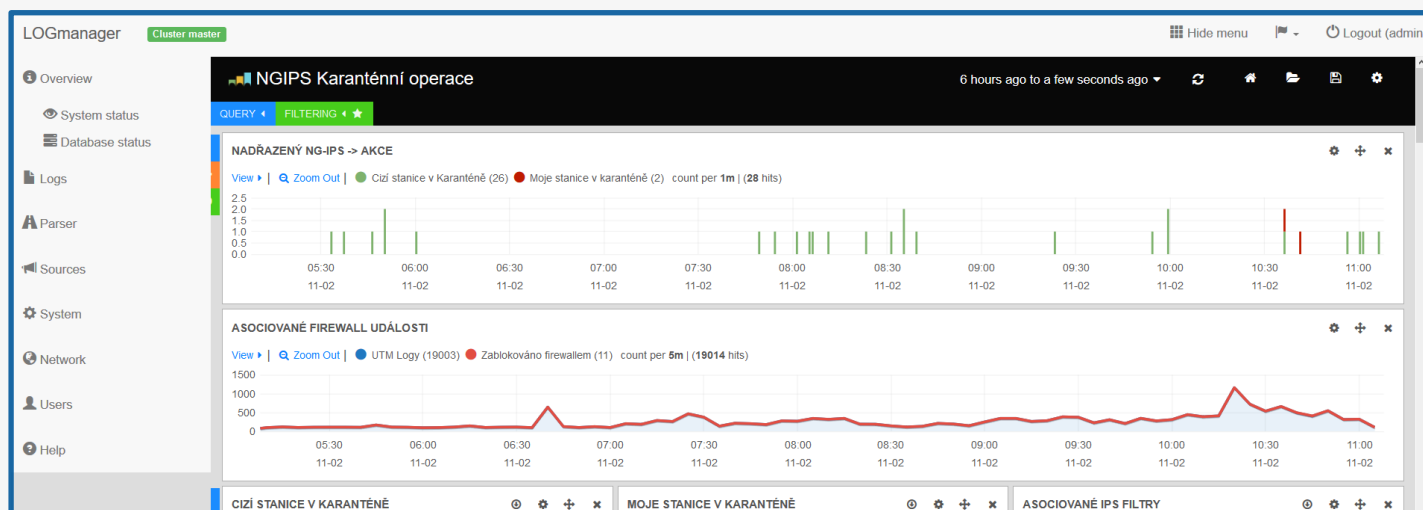


» O zákazníkovi

Nemocnice Jihlava je příspěvkovou organizací, jejímž zřizovatelem je Kraj Vysočina. Jedná se o největší nemocnici v kraji s počtem více než 1.500 zaměstnanců. Je spádovou nemocnicí pro přibližně 200.000 obyvatel, ve vybraných oborech až pro 500.000 obyvatel. Poskytuje 621 akutních lůžek, 75 lůžek následné péče a 10 lůžek paliativní péče. Nemocnice zajišťuje především zdravotní péči, v níž je zahrnuta ambulantní i lůžková diagnostická, léčebná a preventivní péče a lékárenská činnost. Krom toho nemocnice provádí i vědeckou, vzdělávací a informační činnost a ostatní činnosti související s provozováním nemocničního zařízení.

» Rozhodnutí pro nasazení nástroje LOGmanager

Oddělení informačních a komunikačních technologií jihlavské nemocnice má v současnosti na starost několik desítek informačních systémů s tisíci rozličnými HW i SW součástmi. Zákazník v rámci zadání požadoval zajištění sběru informací o funkcích a stavu spravovaných zařízení, zejména bezpečnostních a síťových, a to včetně historie. Hlavním kritériem byla výkonnost zařízení a velikost datového úložiště nabízeného řešení. Zákazník preferoval tuzemský produkt s podporou v českém jazyce. Velkou výhodou LOGmanageru, byla i příznivá cena. Velký SIEM systém nebývá pro společnosti obdobného charakteru ani cenově dosažitelný, ani provozně výhodný – klade totiž velké nároky na čas i odbornost lidské obsluhy. Naproti tomu produkt typu LOGmanager je cenově dostupným řešením, které dokáže splnit vše, co od něj zákazník očekává.



» Rozsah a prezentace projektu

Zákazník kladl největší důraz na zvýšení bezpečnosti své počítačové sítě včetně všech jejích součástí. Od toho se odvíjel průběh implementace. Instalace hardwaru trvala přibližně 4 - 5 hodin, následně proběhlo nastavení prostředí dle požadavků zákazníka, jako první byly řešeny firewally a síťové prvky. Po měsíčním provozu LOGmanageru provedl zadavatel společně s implementátorem doladění systému. V průběhu implementace se zadavatel seznámil s normalizací logů a s alerty, které postupně nasazoval do provozu. Během implementace bylo zaznamenáno mnoho neznámých a těžko identifikovatelných logů, pro které bylo nutné vytvořit pravidla, aby bylo možné informace v nich obsažené efektivně využít. Nasazení LOGmanageru je stále probíhající proces, který se přizpůsobuje rostoucím požadavkům provozu (nárůst dat v prostředí zákazníka se pohybuje v desítkách GB denně) a rozvoji i změnám prostředí. LOGmanager se v prostředí Nemocnice Jihlava ukázal být dostupným a kvalitním logovacím SW a SIEM systémem.

PŘÍNOS PRO ZÁKAZNÍKA A OCEŇOVANÉ VLASTNOSTI

Zařízení LOGmanager lze jednoduše nasadit do již běžícího provozu pro sběr strojových dat z jakéhokoliv zdrojového systému a v jakékoliv organizaci. Velmi snadná integrace je jednou z předností tohoto produktu.

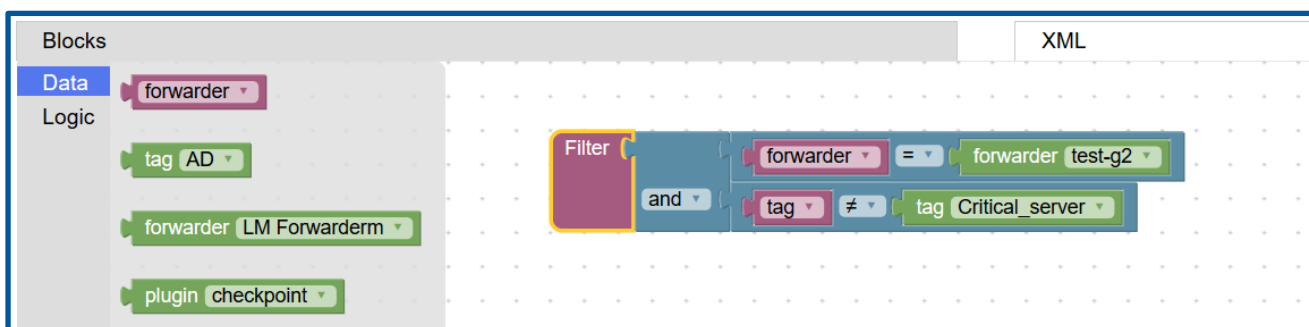
Propojení s různými platformami umožňuje logovat (evidovat) a srozumitelně graficky i textově prezentovat události a logy z libovolných síťových aktivních prvků, bezpečnostních zařízení i operačních systémů a aplikačního software. Jednoduchost a přehlednost zařízení umožňuje poskytovat informace a zasílat alerty dle požadavků administrátorů ICT.

LOGmanager vzhledem ke své rychlosti prohledávání a analýzy logů dokonale splnil očekávání zadavatele. Zákazník také oceňuje jednoduchost upgradu systému a přístup k Webinářům, které obsahují informace o změnách a novinkách i spoustu dalších technických informací od tvůrců LOGmanageru.

Dalším přínosem pro zákazníka je plná dostupnost logů z firewallů a síťových prvků s dlouhodobým uchováním. Nasazením LOGmanageru byly zjištěny bezpečnostní chyby v podobě podvrhnutého DHCP nebo zařízení na síti, která počítala kryptoměnu atp.

» Zákazník oceňuje nejvíce následující vlastnosti

- ⇒ Rychlé nasazení a implementace řešení
- ⇒ Výkon systému a dlouhá retenční doba pro on-line data, možnost snadného zálohování
- ⇒ Snadné nalezení podstaty nefunkčnosti systému který svoje strojová data předává LOGmanageru
- ⇒ Identifikace závad provozního charakteru takřka v reálném čase a automatické upozorňování
- ⇒ Možnost snadno vytvářet vlastní dotazy, grafy, reporty a pohledy v dashboardech LOGmanageru
- ⇒ Rychlé dohledání události popisující příčinu konkrétního problému, ztráty dat nebo výpadku komunikace
- ⇒ Podklady pro vytváření bezpečnostních auditů
- ⇒ Možnosti limitování oprávnění a filtrování zobrazených dat pro neprivilegované uživatele



INFORMACE O VÝROBCI A DALŠÍ REFERENCE

LOGmanager je vyvíjen od roku 2014 jako nosný produkt firmy Sirwisa a.s., která sídlí v Praze. Do vydání tohoto referenčního listu našel LOGmanager více jak 130 spokojených zákazníků a na stránkách www.logmanager.cz naleznete vybrané reference. Mezi naše zákazníky patří nejen státní správa, ale i průmyslové podniky všech velikostí a oborů, obchodní společnosti, společnosti z oblasti bankovníctví a další. Pro podrobnější reference přímo z oblasti Vaší činnosti nás neváhejte popsat. Certifikovaným partnerem realizujícím tento projekt byla firma AUTOCONT a.s..