LOGmanager

> Central Log Repository
> Affordable SIEM

HELP TO RESOLVE CRITICAL IT INCIDENT

LOGmanager - Popis studie proveditelnosti (PoC Test)

Nedílnou součástí každé prodejní příležitosti LOGmanageru je instalace a testování řešení v prostředí zákazníka ve formě PoC (Proof of Concept test). Abychom byli přesní - co se rozumí testem Proof of Concept. LOGmanager PoC je studie proveditelnosti, čili realizace metod nebo nápadů za účelem prokázání vhodnosti nasazení LOGmanageru v prostředí zákazníka. Cílem studie proveditelnosti by v zásadě mělo být ověření, že koncept nasazení LOGmanageru má pro daného zákazníka praktický potenciál. Pamatujte: PoC test je záměrně malý a pokrývá pouze vybrané případy použití zákazníkem (obvykle do pěti) - nenahrazuje implementační službu a plné nasazení LOGmanageru.

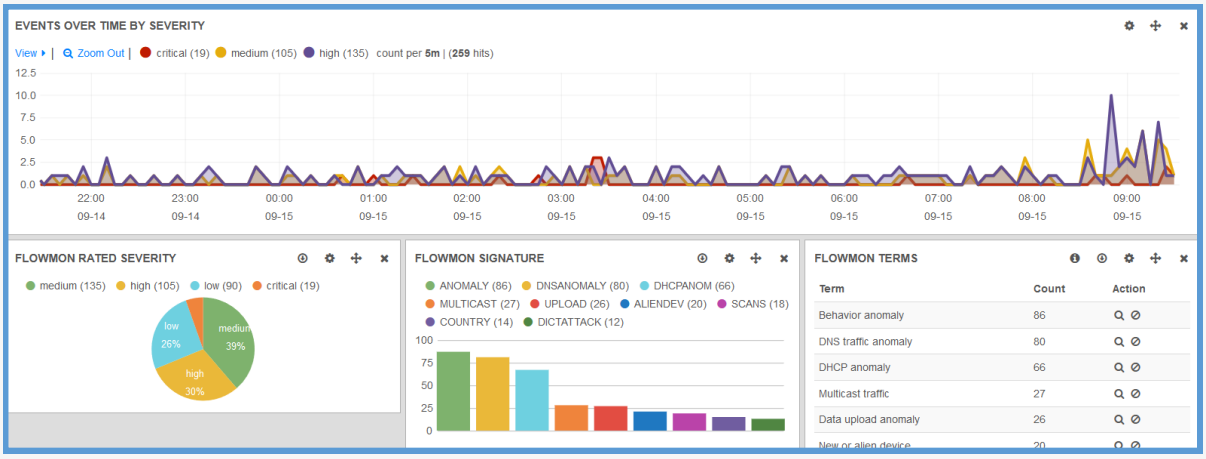
PoC test je poskytován certifikovaným partnerem řešení LOGmanager. Registrovaný partner provádí tuto službu obvykle s podporou specializovaného technika výrobce. Tento datasheet definuje jednotlivé kroky, které je třeba podniknout pro úspěšný průběh PoC, odpovědnosti každé zúčastněné strany, časový plán a check-list instalace.

LOGmanager PoC - Technický pohled

Jak už název napovídá, cílem PoC je prokázat koncepci. V tomto případě je obecnou koncepcí schopnost testovaného systému provádět a poskytovat funkce managementu logů. Jedná se o složité téma, které lze rozdělit do mnoha částí odlišných pro každého klienta. Před provedením PoC si musí všechny zúčastněné strany odsouhlasit, že chápou hlavní úkoly, které by řešení mělo splňovat. Přistoupení k PoC testu bez takové dohody povede k chaotickému a nesmyslnému procesu.

Níže uvádíme několik otázek, které je třeba si položit, abychom porozuměli účelům PoC:

1. **Zaměření / Cíl** - čeho se snažíte dosáhnout? Proč uvažujete o řešení log managementu / SEM / SIEM ve vaší společnosti?
2. **Naléhavost problému** – je pro vás tato záležitost urgentní ve smyslu, že vás neřešený log management stojí peníze?
3. **Úspěšnost** - jak budete měřit úspěch PoC? Přemýšlíte o tom/víte to?
4. **Požadavky** - máte nějaké konkrétní požadavky, které řešení musí splňovat? Specifická omezení, se kterými musíte pracovat, jako jsou zákony, předpisy, směrnice?
5. **Funkcionality** - existují nějaké specifické vlastnosti/funkcionality, které vás zajímají nejvíce? Například - reporty, alerty, korelace, rychlé prohledávání dat, vizualizace dat?
6. **Konkurenční řešení** - máte nějaké předchozí zkušenosti s řešením log managementu? Vyzkoušeli jste jiné produkty, ale rozhodli jste se, že nejsou pro vás? Plánujete testovat i jiné řešení?



Časový plán POC:

LOGmanager PoC test obvykle trvá minimálně dva týdny. Každý PoC test je jiný, takže nelze vypsat přesné kroky, ale na základě našich zkušeností obvykle funguje nejlépe tento níže uvedený plán:

Příprava PoC testu:

1. **Úvodní technická schůzka** – 30 min max – zjištění hlavních problémů, kterým zákazník čelí, a důvodu, proč potřebuje řešit management logů. Cílem je pomoc technikovi připravit demo.
2. **LOGmanager prezentace/demo** – 1 až 2 h – přehled hlavních funkcionalit, jak co řešíme, ukázka produktu se zaměřením na potřeby zákazníka.
3. **Dimenzování a nabídka** - vytvoření nabídky na základě „dimenzovacího“ dokumentu přijatého od zákazníka k zajištění dostatečného rozpočtu pro nákup LOGmanageru v případě úspěšných výsledků PoC testu.
4. **Přípravná schůzka před PoC testem** – 30 min – cílem schůzky je jasně definovat kritéria úspěchu PoC testu.

Vlastní PoC Test:

1. **PoC Instalace** – 2 až 3 h – instalace LOGmanager demo boxu v prostředí klienta a konfigurace základních zdrojů.
2. **PoC Implementace** – 1 až 2 h – konfigurace dalších zdrojů. Nastavení ostatních funkcionalit požadovaných zákazníkem (jako například alertů, korelací, vlastních dashboardů, reportů).
3. **Další schůzky dle potřeby**. Průběžná kontrola průběhu PoC testu.
4. **PoC Shrnutí** – 1 až 2 h – přehled shromážděných dat, prezentace hlavních cílů dle požadavků zákazníka.

POC zodpovědnosti

Každá strana zapojená do PoC má určité povinnosti, které musí splnit, aby byl PoC test úspěšný. Níže jsou uvedeny požadavky na jednotlivé zúčastněné strany:

Zákazník:

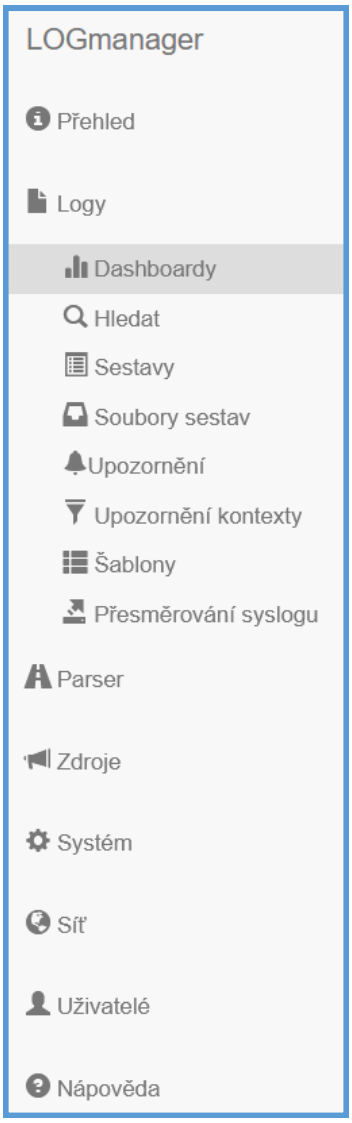
- Definování hlavních cílů PoC testu (spolu s technikem výrobce).
- Poskytnutí jasně definovaných kritérií úspěchu PoC testu.
- Aktivní účast na úvodní technické schůzce.
- Přidělení technika, který bude dohlížet na PoC test podle dohodnutých cílů.
- Splnění instalačních požadavků.
- Vyplnění „dimenzovacího“ dokumentu pro správný návrh rozsahu vhodného řešení.
- V případě, že PoC test probíhá on-site (u zákazníka), rezervace místnosti pro jednání.

Account Manager partnera :

- Pomoc klientovi s definicí úkolů a potřeb daného řešení.
- Přidělení technika, který zajistí vlastní PoC test dle odsouhlasených cílů.
- Odeslání dimenzovacího dokumentu a příprava nabídky.
- Koordinace schůzek a komunikace se zákazníkem.

LOGmanager technik (určený partnerem nebo výrobcem):

- Průběžná konfigurace dalších zdrojů dle požadavků zákazníka, kontrola správnosti klasifikace, parsování a zpracování dat zákazníka.
- Definování a návrhy alertů dle požadavků zákazníka.
- Zaškolení technika přiděleného zákazníkem, zopakování ukázky základních funkcí a vysvětlení pokročilých vlastností systému.
- Vzdálená podpora a konzultace prostřednictvím systému virtuálních schůzek.
- Odladění konfigurace a diagnostika správné činnosti systému.
- Otázky a odpovědi na technické dotazy, pomoc s vytvářením dashboardů, alertů, reportů.
- Vytvoření písemného závěru PoC testu. Po skončení PoC testu – vymazání veškerých zákazníkových dat z LOGmanager PoC demo zařízení.



Požadavky před instalací

Níže je uveden seznam požadavků, které je třeba splnit před instalací. Uvedené informace by měl poskytnout zákazník technikovi LOGmanageru před instalací, aby nasazení LOGmanageru proběhlo hladce. Přílohou tohoto dokumentu je excelová tabulka, kterou je třeba vyplnit dle seznamu níže.

1. **Seznam zdrojů logů, které budou sbírány LOGmanagerem, včetně následujících informací**: Typ zdroje (název výrobce, funkce systému, verze software); Zdrojová IP; Cílový port; Předpokládaný objem logů (pokud je známo).
2. **Informace nezbytné pro zapojení LOGmanageru do sítě:** IP Adresace pro LOGmanager demo systém, včetně: IP adresy; Masky sítě; Defaultní brány; IP adresy primárního DNS; IP adresy sekundárního DNS; NTP serveru.
3. **Konfigurace SMTP přenosů (pro zasílání bezpečnostních a systémových alertů):** IP adresa/Hostname SMTP serveru; Port; Zdrojová emailová adresa (emailová adresa, která se bude ukazovat jako odesílatel); Uživatelské jméno/heslo, pokud je vyžadováno SMTP ověřování; Admin email (emailová adresa, na kterou bude LOGmanager zasílat alerty o interních záležitostech, jako například nedostatečná velikost vyrovnávací paměti).
4. **Je-li požadována integrace s LDAP pro ověřování uživatele:** IP adresa LDAP serveru; IP adresa sekundárního LDAP serveru; LDAP servisní port; Základní struktura adresáře, např. DC=test,DC=example,DC=com; DNS Suffix - např. @test.example.com; Uživatelské jméno/heslo pro přístup k informacím v Active Directory; Seznam LDAP skupin, které mají mít přístup k LOGmanageru.
5. **Bude-li použit WES (LOGmanager windows event sender) agent:** Záznam DNS SRV nastaven podle dokumentace LOGmanager (https://doc.logmanager.cz/manual/3.5.2/cs/devices/microsoft-windows-event-sender.html).

Fyzické požadavky

1. LOGmanager PoC test obvykle probíhá na demo boxu, což je malý Intel NUC (115mm x 111mm x 48.7mm). Potřebuje jen malý prostor na rovném povrchu a jednu 230 V zásuvku, nejlépe takovou, která je zálohována UPS.
2. Ethernetová přípojka pro LOGmanager – 100/1000Base-T k admin VLAN (nebo k VLAN určené k přenosu logovacích dat). Během PoC není nutný přístup k internetu, ale hodí se VPN připojení pro vzdálený přístup LOGmanager technika.

Kontrolní seznam instalace PoC testu

Instalací se myslí úvodní zapojení a zprovoznění LOGmanageru v prostředí zákazníka. Seznámení s pravidly provozu, konfigurace zdrojů logů, událostí a strojových dat, kontrola funkce všech součástí zařízení. Doba potřebná pro instalaci závisí na komplexitě prostředí, obvykle ale nepřesahuje 3 hodiny.

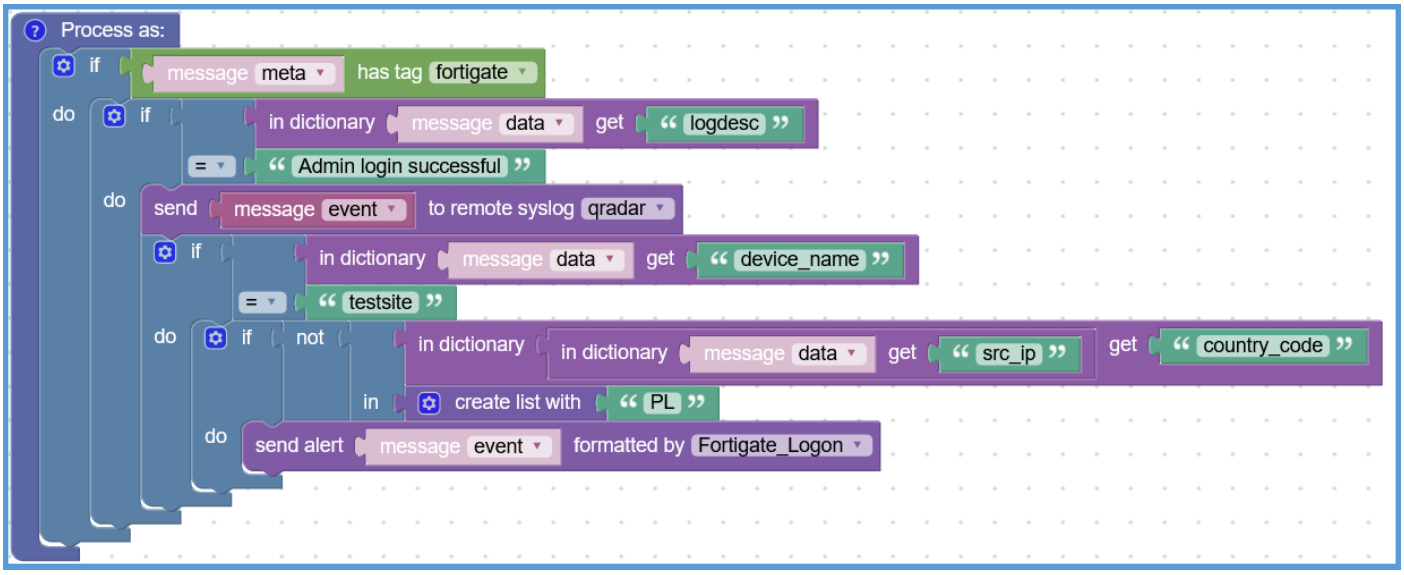
1. Úvodní konfigurace:
    - Připojení Demo Boxu do sítě nastavením poskytnuté konfigurace na primárním rozhraní (IP Adresa, maska sítě, defaultní brána, DNS, NTP).
    - Testování dostupnosti GUI.
    - Testování přístupu k LOGmanager update serveru.
    - Ověření, že Demo Box má nejnovější verzi kódu. Pokud ne, provedení update.
    - Deaktivace automatické telemetrie zasílané výrobci.
    - Konfigurace SMTP nastavení a testování odesílání emailových oznámení.
    - Volitelně:
        - Tvorba skupin uživatelů a nastavení práv pro LOGmanager (ověřování lokálně nebo centralizovaně prostřednictvím AD/LDAP).
        - Pokud je instalován WES agent, konfigurace klientského DNS serveru dle návodu.

2. Přidání podporovaných zdrojů logů a událostí:

   - Ověření, že pro dané zdroje jsou k dispozici klasifikace a parsery. Přidání zdrojové IP do IP Prefix Listu (pokud je třeba). Vytvoření a kontrola správné klasifikace dat.
   - Asistence technikovi zákazníka s konfigurací zdrojových zařízení pro zasílání logů do LOGmanageru.
   - Ověření, že po připojení každého zařízení jsou logy správně sbírány a parsovány (využitím nativních dashboardů pro daný typ zdroje – zda jsou správně zaplněny daty).
   - V případě Windows systémů:
     - Ověření, že je LOGmanager přístupný ze stanice/serveru přes síť na porty 443/20514/20515.
     - Ověření, že SRV záznam je na pracovní stanici správně vyřešen.
     - Instalace WES agenta z MSI souboru dostupného z GUI.
     - Kontrola, že po instalaci byla stanice přidána na Windows Agents List.
     - Konfigurace sběru a filtrování událostí buďto globálně nebo z jednotlivých stanic.
     - Ověření, že jsou logy správně vyčítány z Windows stanic.

3. V případě nepodporovaných zdrojů logů a událostí:

   - Vytvoření správné klasifikace založené na atributech vybraného zdroje (zdrojová IP, cílový port, syslog program name). Nastavení klasifikační akce jako TAG (protože momentálně není dostupný parser).
   - Asistence technikovi zákazníka s konfigurací zdrojového zařízení pro zasílání logů do LOGmanageru.
   - Ověření, že jsou logy správně získávány a značeny na základě vytvořené klasifikace.
   - Export logů do CSV souboru ve formátu RAW.
   - Odeslání vyexportovaného CSV souboru systémovému technikovi výrobce (LOGmanager System Engineer) k vytvoření a základnímu otestování nově vytvořeného parseru.



Návrhy a doporučení k tomuto návodu prosím zasílejte na email adresu: security-team@logmanager.com.

INFORMACE O VÝROBCI A DALŠÍ REFERENCE

LOGmanager je vyvíjen od roku 2014 jako nosný produkt firmy Sirwisa a.s., která sídlí v Praze. 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 bankovnictví a další. Pro podrobnější list referencí přímo z oblasti Vaší činnosti nás neváhejte poptat. Příslušné kontakty na stávající zákazníky, kteří souhlasí s uváděním na referenčním listu, rádi předáme.