

Projektová dokumentace

***„Vybudování JCE IB SOŠ INFORMATIKY A SPOJŮ A SOU
KOLÍN - zpracování projektové dokumentace“***

TECHNOLOGICKÁ ČÁST JCE IB

D.1.4.9. Technologie a řešení JCE IB

D.1.4.9.10. CENTRÁLNÍ LOG MANAGEMENT - ŠKOLA

Zpracoval:

Petr Lacina

10 CENTRÁLNÍ LOG MANAGENEMT (LM) - ŠKOLA

10.1 POPIS

LM umožňuje sběr a vyhodnocení logových informací z jednotlivých prvků infrastruktury, jejich centralizaci a archivaci v jednom místě. Je v souladu s navrhovaným bezpečnostním standardem.

Pro účely kalkulace a návrhu řešení byl použit výpočet potřebných EPS na základě průměrného množství událostí generovaného jednotlivými technologiemi a best practice při napojování zdrojů.

V rámci prostředí Školy bude s ohledem na MBS implementaci LM pro zajišťovat schopnost vyhodnocení logových informací z jednotlivých prvků infrastruktury.

Centrální LM bude provozován v novém virtuálním prostředí školy, které zajistí požadovaný výkon. V rámci realizace tedy není požadována dodávka dalšího hardware.

Škola není povinným subjektem z pohledu zákona o kybernetické bezpečnosti a nevztahují se v tomto ohledu na ni požadavky na dobu uchování dat. Pro účely projektu a alokování kapacit na serverech byla použita doba dostupnosti a uchování dat: 3 měsíce online a dalších 6 měsíců offline.

Servery potřebné pro provoz budou virtualizovány.

10.2 SPECIFIKACE MINIMÁLNÍCH POŽADAVKŮ TECHNICKÉHO ŘEŠENÍ

Log Management je řešením, které umožňuje seskupovat provozní záznamy HW zařízení, OS a aplikací na jednom místě, ve sjednoceném formátu, se zachováním jejich dostupnosti, důvěrnosti a integrity. Díky přehlednému webovému rozhraní pro vyhledávání, přizpůsobitelným reportům a statistikám, umožňuje Log Management snazší práci s logy při analýze, a to jak za účelem auditu, tak i pro zajištění každodenního provozu.

10.2.1 Vlastnosti řešení Log Management

Požadovaná funkcionalita	Specifikace minimálních požadavků
Forma obsluhy	Řešení musí být konfigurovatelné a ovládané přes webové GUI rozhraní.
Počet podporovaných zdrojů log. událostí	1000 IP adres
Komponenta Log Managementu musí mít garantovanou licenci pro:	zpracování 500 EPS nebo 12 GB/day
Provedení	Virtuální appliance: Pro účely navrženého řešení budou zadavatelem poskytnuty zdroje na jeho virtuální platformě.
Podpora zapojení pro High Availability, tj. vysoká dostupnost.	
Podpora vstupních protokolů (sources ~ zdrojů log záznamů) a přenosu dat.	SNMP, syslog: - UDP (dle RFC 3164), - TCP, - IETF (RFC 5424) + TLS
Aktivní sběr logů z databází.	přes ODBC, minimálně MSSQL, MYSQL, ORACLE
Podpora BUFFER/CACHE na výstupu jak u Agentu, tak pro RELAY, a také pro Server/Appliance.	
Podpora výstupních protokolů (destinations ~ umístění log záznamů).	syslog (UDP, TCP, IETF). zápis logových dat napřímo do databází (ODBC). zápis logových dat do JSON formátu. SNMP Trap.
Řízení přístupů (AAA) - řízení přístupu na úrovni jednotlivých úložišť (logspace).	
Zálohování, Archivace, Export, Sdílení log dat	Nezávislé zálohovací politiky jak pro konfiguraci, tak pro jednotlivá úložiště (logspace). Nezávislé archivační (data retention) politiky pro jednotlivá úložiště log dat. Podpora exportu/sdílení log dat v originálním i ve strukturovaném tvaru.

Řešení není provázáno na SIEM a je plně nezávislé jak fyzicky tak logicky na SIEM řešeních.	Nejedná se tedy o ALL-IN-ONE řešení, s konfigurací pro Log Management.
Rychlé vyhledávání na základě fulltext indexace (vyhledávání bez nutnosti tvorby parserů).	Velké objemy dat se neprohledávají formou „grep like“ prohledávání po řádcích.
Peering - možnost propojit více Log Management serverů a vyhledávání nad nimi přes jedno rozhraní.	Podpora minimálně 20 peerů.
Peering - definice vyhledávacích filtrů a „pohledů“ nad „peeringovými“ servery. Podpora přístupů pro pohledy (co pohled to jiná skupina uživatelů).	Podpora minimálně 20 peerů.
Možnost vyhledávání přes REST API rozhraní.	
Všechny potřebné komponenty HW i SW musí být součástí dodaného systému LM, včetně databáze.	
Log Management je fyzicky i logicky nezávislý na SIEMu. Při nedostupnosti SIEMu je Log Management plně funkční a obsahuje všechny logy v RAW formátu. Při nedostupnosti Log Managementu je SIEM plně funkční a obsahuje všechny potřebné logy v normalizovaném formátu. Vrstva zajišťující sběr je fyzicky i logicky nezávislá na LM a SIEM. Při nedostupnosti jak SIEM tak LM vrstva nadále funguje nezávisle a zajišťuje jak sběr logů tak je možné ji konfigurovat.	
Log Management je rámci celkového řešení integrován se SIEM. Je tedy možné se ze SIEM konzole překlikem („dril down“) dostat do Log Managementu.	
Všechny požadované funkce se spravují a využívají přes společnou řídicí konzoli (dále jen „Centrální správa“), která je rovněž přístupná přes webové rozhraní z fyzického i virtuálního PC s využitím Internet Exploreru 11.0 a novějších, nebo jiným podobným způsobem. Prezentace dat musí být provedena v grafické podobě, prezentační rozhraní musí být multiplatformní nebo platformě nezávislé a plně funkční na platformách Windows, Linux, Apple OS.X.	
Systém LM musí umožňovat přihlašování pomocí lokálních účtů pro případ neaktivního propojení s AD.	
Řešení musí umožnit přístup více uživatelů současně, a to jak na úrovni přístupu ke vstupním/zdrojovým datům systému, tak i k incidentům. Přístup uživatelů musí být založen na volně definovaných, oddělených rolích s možností granulárního přidělování práv v rámci každé role, dle zdrojových dat, identifikace monitorovaných zařízení, skupin zařízení a serverů, typu vstupních dat, apod. Role nesmí být vázány na AD, musí být spravovány interně.	
Řešení musí podporovat nebo být rozšiřitelné pro kompletní oddělení skupin uživatelů k odlišným datům a konfiguracím, kdy jednotlivé instance mohou mít možnost vlastní konfigurace	

a správy (multi-tenant přístup) a samostatných oddělených logspace.	
Řešení musí nativně podporovat protokoly IPv4, IPv6, jak při normalizaci vstupních dat, tak i při komunikaci se zdroji dat.	
Systém LM musí mít srozumitelně a prokazatelně deklarováno vedení licenční politiky, a to včetně uvedení funkcionalit, které nejsou součástí základní licence a zda a za jakých podmínek je možné je dokupovat.	
Komponenta sbírající logy, musí být schopna trvale zpracovávat 10000 EPS bez jakýchkoliv výkonnostních nebo licenčních omezení.	
Komponenta Log Managementu musí mít garantovaný výkon pro zpracování 10000 EPS.	
Systém dále musí umožnit uchovávání logů formou záloh a zejména musí umožnit obnovení vybraných částí logů a jejich zpřístupnění přes Centrální správu LM.	
Licence musí obsahovat možnost minimálně 1000 sběrných konektorů, včetně vlastních custom logů (možnost doplnit další lokality, zdroje událostí, atd).	
Licence musí obsahovat možnost sbírat všechny typy výrobcem podporovaných zdrojů událostí a vlastních custom logů.	
Vrstva sběru logů musí podporovat načítání log souborů (jedno a víceřádkové textové logy), kde tyto soubory budou mít stanovenou strukturu a význam dat.	
Vrstva sběru logů musí podporovat načítání logů z databáze (zejména Microsoft SQL a Oracle), kde tyto logy budou mít stanovenou strukturu a význam dat.	
Vrstva sběru logů musí umožňovat načtení a zpracování jakýchkoli typů logů, i z vlastních aplikací, tato možnost musí být k dispozici bez součinnosti výrobce nebo dodavatele řešení. Kvalita výstupu a možnosti využití musí být stejné jako v případě standardně podporovaného zdroje logů.	
Komponenta sbírající logy je musí posílat dále zašifrované a komprimované a musí umožňovat regulovat šířku užívaného pásma.	
LM systém musí podporovat pravidelné automatické přesuny dat z interního do externího úložiště, resp. archivu podle definovaných pravidel, a bez vzniku neautorizovaných změn dat;	
LM musí ukládat data v komprimované podobě pro úsporu diskové kapacity, a to v rámci interního i externího úložiště;	
LM systém musí umožňovat snadnou obnovu historických dat z archivů pro zpětnou analýzu;	

LM systém musí poskytovat mechanismus detekce neautorizovaných změn dat (kontrola integrity) v souborech systému LM;	
Systém LM musí poskytovat reporty i ve formě grafů a tabulek.	
Systém LM musí vytvářet reporty ve formátech PDF, HTML a CSV, popř. dalších.	
Systém LM musí obsahovat analytické nástroje umožňující např. reportování, forenzní analýzu, analýzu změn, statistické reporty nad aktuálními i historickými daty.	
Systém LM musí podporovat možnost zobrazit Log záznam v původní formě, jak byl přijat, tzn. raw-message.	
Systém LM musí podporovat automatické spouštění definovaných reportů (měsíčně, týdně, denně, nebo v definovaném čase), ukládání na síťové úložiště a jejich zasílání e-mailem přímo ze systému.	
Řešení poskytuje funkci event. managementu (práce s událostmi ve formě strukturovaných eventů)	Součástí dodávky je sada parserů pro obvyklá zařízení klasických ICT výrobců
Vrstva sběru (zpracování, parsování, normalizace,...) je logicky i fyzicky oddělená od centrální komponenty LM (server zajišťující uložení a vyhledávání)	
Záruka a servisní podpora	Požadujeme dodání řešení vč. supportu/servisní podpory na dobu 5 let. Podpora musí zahrnovat všechny updaty i upgrady, telefonická nebo emailová podpora výrobce v rozsahu alespoň 8x5.