

KUPNÍ SMLOUVA

uzavřená podle § 2079 a násl. zákona č. 89/2012 Sb., občanský zákoník (dále jen „občanský zákoník“) mezi níže uvedenými smluvními stranami:

strana:	Kupující	Prodávající
název / firma:	Psychiatrická nemocnice Bohnice	Caleum a.s.
sídlo:	Ústavní 91, 181 02 Praha	Na Pankráci 1724/129, 140 00 Praha
IČ / DIČ:	00064220 / CZ00064220	28351363 / CZ28351363
registrace:		
oprávnění smluvních:	MUDr. Martin Hollý, MBA - ředitel	Josef Ladra, předseda představenstva
jednat ve věcech	technických (realizačních): Ing. Josef Lukeš, Ph.D. – vedoucí odboru ICT	David Horn , System architect
osoba oprávněná předat / převzít předmět smlouvy	Ing. Josef Lukeš, Ph.D.	Jiřina Bastlová, Key Account Manager
bankovní spojení:	16434081/0100	107-2149840277/0100
tel./e-mail/datová schr.:	██████████	██████████
číslo smlouvy:		202103 LM PNB

Čl. 1

Předmět plnění

- 1.1 Předmětem plnění je dodávka věcí, činností a dalších souvisejících plnění dle specifikace uvedené v Příloze č. 1 této smlouvy (dále jen „předmět koupě“). Přesná specifikace předmětu koupě je uvedena v Příloze č. 1, která tvoří nedílnou součást této smlouvy.
- 1.2 Podkladem pro uzavření této smlouvy je nabídka prodávajícího ze dne 24.2.2021 (dále jen „nabídka“) podaná ve veřejné zakázce „**Návrh, dodání a implementace centrálního úložiště pro sběr a analýzu logů a událostí z kritických systémů, serverů a aplikací zadavatele**“, (dále jen také „Zakázka“) zadávané jak zakázka malého rozsahu.
- 1.3 Závaznou součástí této smlouvy, ač k ní pevně jako její příloha vzhledem k jejímu rozsahu nepřipojena, je také zadávací dokumentace kupujícího (coby zadavatele Zakázky) pro Zakázku ve znění případných pozdějších úprav a upřesnění, např. po žádostech o dodatečné informace, (dále také jen „Zadávací dokumentace“). Podkladem pro uzavření této smlouvy je pak také shora uvedená nabídka prodávajícího (coby účastníka, resp. vybraného dodavatele Zakázky). Nabídka prodávajícího je také závaznou součástí této smlouvy a podkladem pro její uzavření, ač k ní také není vzhledem k jejímu rozsahu pevně připojena, jako její příloha. V případě rozporu Nabídky prodávajícího s podklady kupujícího (zejm. se Zadávací dokumentací), mají přednost podklady kupujícího.
- 1.4 Touto kupní smlouvou se prodávající zavazuje, že kupujícímu odevzdá předmětem koupě, a umožní mu nabýt vlastnické právo k němu, a kupující se zavazuje, že jej převezme a zaplatí prodávajícímu kupní cenu.
- 1.5 Součástí předmětu plnění podle této smlouvy je a prodávající se zavazuje provést také nezbytnou montáž, nastavení, aj. práce a činnosti nutné k zajištění řádného a kupujícím požadovaného fungování předmětu koupě. Součástí plnění podle této smlouvy je dále také závazek prodávajícího dodat veškeré doklady vztahující se k řádnému užívání předmětu plnění a veškeré doklady požadované právními předpisy k používání předmětu koupě. Prodávající prohlašuje, že předmět koupě splňuje veškeré podmínky stanovené příslušnými právními předpisy a technickými normami k používání předmětu koupě, a že kupujícímu předá veškeré doklady potřebné k provozování předmětu koupě, za což kupujícímu ručí.
- 1.6 Předmětem plnění podle této smlouvy a závazkem prodávajícího je dále poskytování bezplatného servisu po dobu celé **záruční lhůty** uvedené v čl. 6.1 této smlouvy, za podmínek uvedených dále a minimálně v rozsahu stanoveném výrobcem příslušného předmětu koupě včetně oprav a dodávky náhradních dílů, a to vše tak, aby byl předmět koupě minimálně po dobu záruční doby plně funkční a provozuschopný a plnil svůj účel, k němuž je určen a kupujícím požadován. Pokud se týče SW, prodávající pak dále zajistí také podporu výrobce na aktualizaci systému a parserů po dobu celé záruční lhůty, která musí obsahovat aktualizaci SW minimálně 4x ročně, opravy chyb a telefonickou a emailovou podporu s diagnostikou vzdáleným přístupem.

- 1.7 V případě, že bude při provádění díla potřeba poskytnutí licence, Prodávající je povinen poskytnout Objednateli uživatelskou licenci k příslušnému zadavatelem požadovanému a/nebo nutnému k řádnému fungování předmětu plnění softwaru dle této Smlouvy; za tím účelem se zavazuje uzavřít příslušnou smlouvu, bude-li to třeba s tím, že cena takové licence je již zahrnuta v dále uvedené kupní ceně. Prodávající dále prohlašuje, že poskytnutím licence Kupujícímu neporušuje práva duševního vlastnictví třetích osob a že nejsou třetí osoby, které by mohly oprávněně uplatňovat své nároky z těchto práv vůči Kupujícímu. V případě, že Prodávající nedodrží toto ustanovení, zavazuje se uhradit veškeré nároky třetích osob z důvodu porušení práv duševního vlastnictví třetích osob a dále náhradu škody způsobenou tím Kupujícímu. Prodávající rovněž poskytuje Kupujícímu vlastnické právo k instalačním médiím, na nichž je Software poskytován a k dalšímu příslušenství (návody v jakékoli podobě, hardwarové klíče apod.). Instalačním médiem se rozumí flash paměť (flash disk), magnetické diskové paměťové jednotky (přenosné disky) a médium pro ukládání dat (cd-rom,dvd-rom).

Čl. 2

Kupní cena, platební podmínky

- 2.1 Kupní cena za předmět plnění uvedený v této smlouvě činí celkem **849.250,- Kč bez DPH**. DPH ve výši 21 % činí **178.342,50 Kč**. Celková cena včetně DPH ve výši 21 % činí **1.027.592,50 Kč** (slovy: jedenmiliondvacetsedmtisícpětsetdevašátdva korun českých a padesát haléřů). DPH bude účtována dle platných právních předpisů. V ceně dle tohoto odstavce jsou vedle dodání předmětu plnění zahrnuty zejm. instalace, zprovoznění, balné a doprava až na místo dodání. Sjednaná cena celkem může být změněna pouze a jen, pokud po podpisu smlouvy a před dodáním dojde ke změnám sazeb DPH předmětu plnění dle této smlouvy.
- 2.2 Dodavatel je plátcem DPH.
- 2.3 Kupní cena je stanovena jako nejvýše přípustná a konečná a zahrnuje celý předmět plnění této smlouvy včetně případných licencí uvedených v čl. 1. této smlouvy.
- 2.4 Prodávající vystaví jednu konečnou fakturu, a to po dodání předmětu koupě. Přitom platí, že součástí faktur musí být předávací protokol potvrzený kupujícími.
- 2.5 Daňový doklad (faktura) vystavený prodávajícím v souladu s touto smlouvou musí být vystaven v korunách českých a být doručen na adresu kupujícího uvedenou v záhlaví této smlouvy. Daňový doklad musí mít náležitosti stanovené platnými právními předpisy. Na daňovém dokladu musí být uvedeno registrační číslo projektu, ze kterého bude provedena úhrada dle této smlouvy. Daňový doklad, který nebude mít požadované náležitosti, je kupující oprávněn vrátit ve lhůtě splatnosti prodávajícímu k opravě. V takovém případě začne běžet nová lhůta splatnosti doručením opravené (doplněné) faktury kupujícímu.
- 2.6 Splatnost daňového dokladu je stanovena na 30 kalendářních dní od jeho doručení kupujícímu na adresu uvedenou v záhlaví této smlouvy. Fakturovaná částka je uhrazena dnem připsání částky na účet prodávajícího.
- 2.7 Všechny platby ve prospěch prodávajícího dle této smlouvy budou činěny bezhotovostně na účet prodávajícího uvedený na příslušném daňovém dokladu příp. v této smlouvě s níže uvedenými výjimkami.
- 2.7.1 Smluvní strany se dohodly, že příjemce zdanitelného plnění (dále též jen „příjemce“) je oprávněn uhradit za poskytovatele zdanitelného plnění (dále též jen „poskytovatel“) daň z přidané hodnoty z takového zdanitelného plnění v souladu s § 109a ZDPH, pokud je v okamžiku uskutečnění zdanitelného plnění o poskytovateli zveřejněna způsobem umožňujícím dálkový přístup skutečnost, že je nespolehlivým plátcem.
- 2.7.2 Dále se smluvní strany dohodly, že příjemce je oprávněn uhradit za poskytovatele daň z přidané hodnoty z takového zdanitelného plnění v souladu s § 109a ZDPH také v případě: (i) kdy má být peněžní plnění poskytnuto bezhotovostním převodem zcela nebo zčásti na účet vedený poskytovatelem platebních služeb mimo Českou republiku, nebo (ii) kdy poskytovatel nesplní dohodnutou povinnost, tedy, že účet, na který má být příjemcem peněžní plnění poskytnuto, nebude po celou dobu splatností peněžního závazku správcem daně zveřejněn způsobem umožňujícím dálkový přístup, a pokud úplata za toto plnění překračuje dvojnásobek částky podle zákona upravujícího omezení plateb v hotovosti, při jejímž překročení je stanovena povinnost provést platbu bezhotovostně (§ 4 zák. č. 254 /2004 Sb.), nebo (iii) ostatních případů ručení příjemce podle § 109 ZDPH.
- 2.7.3 Smluvní strany shodně prohlašují, že uhrazení částky odpovídající výši daně z přidané hodnoty na účet správce daně za poskytovatele bude považováno v tomto rozsahu za splnění závazku příjemce uhradit peněžní závazek poskytovateli.

- 2.7.4 Smluvní strany se dohodly, a poskytovatel s tím souhlasí a zavazuje se, že nijak nepřevéde na třetí osobu ani nijak nezatíží vůči třetí osobě jakékoli peněžní pohledávky za příjemcem vyplývající z této smlouvy a/nebo s ní jakkoli související do okamžiku jejich splatnosti.
- 2.8 Smluvní strany se dále dohodly, že pokud prodávající pověří plněním smlouvy nebo její části třetí osobu (poddodavatele), zavazuje se řádně a včas proplácet oprávněně vystavené faktury poddodavatelů za podmínek ve smlouvách s nimi sjednanými, kdy za řádné a včasné plnění se považuje plné uhrazení poddodavatelem vystavených faktur za poskytnutá plnění, a to vždy do 3 pracovních dnů od obdržení platby ze strany kupujícího za konkrétní plnění. Kupující má právo si smlouvy s poddodavatelem vyžádat, stejně jako doložení, že úhrady poddodavatelům byly provedeny řádně a včas, prodávající je povinen mu kontrolu umožnit a prokázat splnění uvedených povinností. Proávající je povinen také zajistit sjednání a dodržování smluvních podmínek se svými poddodavatelem srovnatelných s podmínkami sjednanými v této smlouvě, a to zejména ve vztahu k výši smluvních pokut a délce záruční doby. Uvedené smluvní podmínky se považují za srovnatelné, bude-li výše smluvních pokut a délka záruční doby shodná s úpravou dle této smlouvy. Kupující má právo si smlouvy s poddodavatelem vyžádat a prodávající je povinen mu kontrolu smluv umožnit a prokázat splnění uvedených povinností (§ 6 odst. 4 ZZZVZ).
- 2.9 Při nesplnění povinností (dle odst. 2.8) umožnit kupujícímu kontrolu a/nebo doložit splnění příslušné povinnosti prodávajícím má kupující právo na smluvní pokutu ve výši 5000,- Kč za každý jednotlivý případ porušení kterékoli uvedené povinnosti (§ 6 odst. 4 ZZZVZ).

Čl. 3

Povinnosti prodávajícího, doba a místo plnění

- 3.1 Proávající bude informovat kupujícího alespoň e-mailem minimálně 3 pracovní dny předem o termínu dodání předmětu koupě.
- 3.2 Předmět koupě uvedený v článku č. 1 této smlouvy prodávající dodá nejdéle do 2 měsíců od uzavření této smlouvy. Předmět koupě musí být nový a nepoužitý.
- 3.3 Místo dodání jednotlivých zkompletovaných logických celků je: sídlo kupujícího. Dodávka se považuje za splněnou předáním a převzetím posledního logického celku předmětu plnění.
- 3.4 Po splnění dodávky každého jednotlivého logického celku v rozsahu stanoveném v této smlouvě bude vyhotoven zápis o předání a převzetí předmětu koupě (dále také jen „Předávací protokol“), který bude obsahovat níže uvedené náležitosti:
- označení dodacího listu – zápisu o předání a převzetí předmětu koupě,
 - název a sídlo prodávajícího a kupujícího,
 - označení kupní smlouvy,
 - označení dodaného předmětu plnění včetně výrobních čísel.
- 3.5 Předávací protokol podepíše oprávněný zástupce obou smluvních stran, přičemž jeho podpisem dochází k převzetí a předání zboží a ke splnění definované části (logického celku) předmětu dodávky.
- 3.6 Proávající umožní kupujícímu konzultaci problémů v českém jazyce po telefonu.
- 3.7 Proávající se zavazuje, že po dobu záruční doby bude zajišťovat záruční servis k předmětu koupě dle této smlouvy a garantuje dostupnost servisu a plného sortimentu náhradních dílů.
- 3.8 Zhotovitel se tedy zavazuje poskytovat jakékoliv plnění dle této Smlouvy na vysoké odborné úrovni, v souladu s pokyny kupujícího, platnými právními předpisy, českými státními normami (ČSN), které se týkají předmětu této smlouvy, jakož i nařízením a obecně závaznými vyhláškami. Proávající je povinen poskytovat plnění v co nejvyšší míře tak, aby odpovídalo, je-li to objektivně možné, nejnovějším technologickým trendům a inovativním poznatkům (§ 6 odst. 4 ZZZVZ).

Čl. 4

Povinnosti kupujícího

- 4.1 Kupující je povinen zaplatit kupní cenu podle článku II. této smlouvy a převzít předmět koupě dle této smlouvy.
- 4.2 Kupující není povinen převzít kteroukoliv část předmětu plnění, pokud prodávající neprokáže, že její technické parametry odpovídají hodnotám, resp. příloze č. 1 – specifikaci předmětu koupě.
- 4.3 Kupující poskytne prodávajícímu potřebnou součinnost při plnění podle této smlouvy.

Čl. 5

Odstoupení od smlouvy

- 5.1. Smluvní strany mohou odstoupit od smlouvy, případně jen od její části – příslušného předmětu plnění, v případě jejího podstatného porušení druhou smluvní stranou, přičemž podstatným porušením smlouvy se rozumí zejména:
- předmět této smlouvy není dodán v takovém provedení, tak jak je uvedeno v této smlouvě, nebo technické parametry neodpovídají zadávací dokumentaci
 - prodávající překročí dodací lhůtu uvedenou v čl. 3., odst. 3.2 o více jak 15 pracovních dní.

Čl. 6

Odpovědnost za vady, záruka za jakost

- 6.1. Prodávající poskytuje tímto kupujícímu vedle práv z vadného plnění také záruku za jakost podle § 2113 obč. zák. a to v délce 5 let na HW a 3 roky na SW. Prodávající se zavazuje, že předmět koupě dodaný na základě této smlouvy bude nový a nepoužitý, po záruční dobu způsobilý pro použití k účelu požadovanému kupujícím a k účelu, ke kterému je určen, bude mít vlastnosti požadované kupujícím, touto smlouvou, právními předpisy, jakož i platnými technickými normami, předpisy, směrnici a vyhláškami, a že si tyto vlastnosti beze změny zachová s přihlédnutím k běžnému opotřebení a omezené životnosti komponent spotřebního charakteru.
- 6.2. Prodávající se zavazuje, že se v případě reklamace předmětu koupě, resp. po celou záruční dobu se dostaví nejpozději následující pracovní den od oznámení reklamace ke kupujícímu za účelem vyřízení reklamace.
- 6.2.1. Prodávající se zavazuje přednostně vyřídit reklamaci (provést opravu, údržbu, apod.) v místě instalace. Pokud nebude možné vyřídit reklamaci na místě u kupujícího, tak se prodávající zavazuje, že si převezme reklamovaný předmět koupě od kupujícího v jeho sídle a zajistí vyřízení reklamace v souladu s požadavkem kupujícího a občanským zákoníkem.
- 6.2.2. Pro případ, že se prodávající nedostaví ke kupujícímu ani následující den po marném uplynutí shora uvedené lhůty, má kupující právo zajistit si vyřízení reklamace sám, avšak na náklady prodávajícího; tím není dotčeno právo kupujícího na náhradu případně vzniklé škody, ke které je prodávající povinen vedle úhrady nákladů na vyřízení reklamace, ani záruka poskytnutá prodávajícím, resp. jeho odpovědnost za vady.
- 6.3. Prodávající se zavazuje, že reklamaci vyřídí a dodá reklamovaný předmět koupě (případně nový podle způsobu vyřízení reklamace) kupujícímu ve lhůtě nejpozději do 30 dnů od oznámení reklamace.
- 6.3.1. Pro případ, že prodávající nevyřídí reklamaci ve lhůtě 45 dnů od oznámení reklamace, má kupující právo kdykoli od následujícího dne dále od smlouvy stran reklamovaného předmětu koupě odstoupit.
- 6.3.2. Pro případ, že prodávající nevyřídí reklamaci ve shora uvedené lhůtě 30 dnů, má dále kupující od 31. dne včetně právo na smluvní pokutu ve výši 200,- Kč za každý i započatý den prodlení. Pro případ, že prodávající nevyřídí reklamaci ani do 40 dnů od oznámení reklamace, má dále vedle smluvní pokuty podle věty první (ve výši 500,- Kč za každý i započatý den prodlení) kupující právo na jednorázovou smluvní pokutu ve výši 5000,- Kč. V případě, že dojde k odstoupení od smlouvy dle odst. 6. 4., má kupující právo na smluvní pokutu podle věty první (ve výši 200,- Kč za každý i započatý den prodlení) až do 45. dne včetně od oznámení reklamace.
- 6.4. Kupující má právo od smlouvy stran příslušného předmětu koupě odstoupit, pokud se na něm projeví jakékoli tři vady (nemusí se jednat vždy o stejné vady), resp. pokud již kupující příslušný předmět koupě dvakrát reklamoval.
- 6.5. Záruční servis se zavazuje prodávající poskytovat bezplatně v záruční době a na celou dodávku předmětu plnění. Bezplatný záruční servis pokrývá veškeré náklady na náhradní díly, případně cestovné a práci servisních techniků nebo dopravu přístroje od kupujícího do servisního střediska a zpět.
- 6.6. Prodávající pro účely oznámení vadného plnění (reklamace) poskytne jedno telefonní číslo a jednu e-mailovou adresu, které budou v případě potřeby aktualizovány:
Telefon: + [REDACTED]
- 6.7. Kupující je povinen ohlásit prodávajícímu jakékoli vady předmětu koupě neprodleně poté, co je zjistí, a to telefonicky a e-mailem na shora uvedené kontakty.
- 6.8. Prodávající se zavazuje, že kupujícímu poskytne pozáruční servis a dostupnost servisu (včetně náhradních dílů) nejméně po dobu 36 měsíců od konce záruční doby v rozsahu záručního servisu.

Čl. 7

Sankční ujednání

- 7.1. Smluvními stranami bylo ujednáno, že pokud bude kupující v prodlení s úhradou ceny plnění ujednané podle této smlouvy, je kupující povinen zaplatit úrok z prodlení ve výši stanovené příslušným právním předpisem.
- 7.2. Ocitne-li se prodávající v prodlení s plněním, a to i jen z části, resp. kteréhokoli plnění dle této smlouvy, je povinen zaplatit kupujícímu smluvní pokutu ve výši 0,3 % Kč z kupní ceny konkrétního (včas nedodaného) předmětu plnění, s nímž je v prodlení, za každý byt' započatý kalendářní den prodlení se splněním dodávky.
- 7.3. Smluvní pokuty je kupující oprávněn započítat proti pohledávce prodávajícího.
- 7.4. Zaplacením smluvních pokut podle této smlouvy není dotčeno právo na náhradu škody v celém jejím rozsahu, ani splnění povinností smluvní pokutou utvrzené.

Čl. 8

Ostatní ujednání

- 8.1. Tato smlouva nabývá platnosti podpisu oprávněnými zástupci obou smluvních stran a účinnosti dnem zveřejnění v registru smluv.
- 8.2. Tato smlouva podléhá zveřejnění v registru smluv ve smyslu zák. č. 340/2015 Sb., o registru smluv, v platném znění. Tato smlouva nabývá platnosti dnem jejího podpisu oprávněnými zástupci obou smluvních stran a účinnosti dnem jejího zveřejnění v registru smluv. Zveřejnění této smlouvy v registru smluv zajistí objednatel. Dodavatel je povinen zadavateli sdělit, obsahují-li dokumenty předložené v rámci zadávacího řízení a při uzavření smlouvy o dílo informace, které se podle příslušných právních předpisů neuveřejňují.
- 8.3. Smluvní strany se dohodly, že vlastnické právo k dodanému předmětu plnění dle této smlouvy nabývá kupující okamžikem bezvýhradného podpisu Předávacího protokolu. Tímto okamžikem přechází riziko nahodilé zkázy na kupujícího.
- 8.4. Jakékoli změny či dodatky, kterými se mění nebo ruší tato smlouva nebo její část, jsou platné pouze ve formě písemných dodatků ke smlouvě podepsaných oprávněnými zástupci smluvních stran. Písemná forma platí i pro změny tohoto ustanovení odst. 8.4.
- 8.5. Právní vztahy touto smlouvou neupravené, jakož i právní poměry z ní vznikající a vyplývající, se řídí příslušnými ustanoveními zák. č. 89/2012 Sb., občanský zákoník a dalšími právními předpisy České republiky.
- 8.6. Ujednává se, že případné spory vzniklé z této smlouvy budou účastníci řešit především vzájemnou dohodou. Pro řízení o případných sporných nárocích se ujednává příslušnost obecních soudů. Rozhodným právem je právo České republiky.
- 8.7. Nedílnou součástí této smlouvy je příloha č. 1 – specifikace předmětu koupě.
- 8.8. Tato smlouva je vyhotovena ve třech stejnopisech. Kupující obdrží dva a prodávající jeden stejnopis.
- 8.9. Smluvní strany prohlašují, že si tuto smlouvu před jejím podpisem řádně přečetly, s jejím obsahem souhlasí a na důkaz toho jí stvrzují vlastnoručním podpisem oprávněnými zástupci obou smluvních stran.

V Praze, dne

V Praze, dne 30. března 2021

.....
Psychiatrická nemocnice Bohnice
MUDr. Martin Hollý, MBA, ředitel

.....
Caleum a.s.
Josef Ladra, předseda představenstva

Příloha č. 1 - Specifikace předmětu koupě

Níže je uvedena Specifikace výrobku tak, jak byla popsána v nabídce uchazeče:

Společnost Caleum a.s. nabízí v souladu s požadavky uvedenými v Zadávací dokumentaci LOGmanager-L s velikostí databáze 40 TB včetně 5-leté servisní podpory na hardware appliance s opravou v místě instalace serveru a s garantovanou odezvou následující pracovní den od nahlášení případné závady a podporou výrobce na aktualizaci systému a parserů na 3 roky. Podpora obsahuje aktualizaci SW minimálně 4x ročně, opravy chyb, telefonickou a emailovou podporu s diagnostikou vzdáleným přístupem.

Nabízené řešení splňuje veškeré požadavky Zadavatele uvedené v Zadávací dokumentaci.

LOGMANAGER

V dnešním přetechizovaném světě jsou informace kritickým zdrojem umožňujícím správné rozhodnutí ve správný čas. V protikladu k tomuto konstatování stojí fakt, že důležité informace jsou distribuovány v nejrůznějších zařízeních a aplikacích napříč celou organizací, ne vždy ve snadno pochopitelném formátu a s rozdílnou dostupností. Sjednocení informací z mnoha zdrojů a jejich přeložení do lidsky srozumitelného tvaru, nastavení pevných pravidel pro nakládání s informacemi a jejich nezpochybnitelnost jsou proto klíčové požadavky pro efektivitu bezpečnostních i operativních činností každé organizace. Když se k tomu přidá i přehledná interpretace těchto informací v kompaktním a výkonném nástroji, získá IT organizace pořízením systému LOGmanager nástroj pro realizaci důležitých rozhodnutí.

URČENÍ SYSTÉMU LOGMANAGER

LOGmanager je HW řešení pro centralizovanou správu logů a jiných strojových dat z libovolných zdrojů. Je založen na výkonné databázi s obrovskou kapacitou, rychlým vyhledáváním ve "velkých datech" a okamžitou vizualizací vyžádaných dat. Jeho podstatou je sběr, dlouhodobé nezpochybnitelné ukládání a analýza strojových dat organizace. Umožňuje prohledávat agregovaná data v reálném čase, vytvářet analýzy, reporty a upozornění na události korelované z dat více zdrojů. Nedílnou součástí řešení LOGmanager je taktéž podpora souladu s požadavky zákonných norem. Při správné implementaci pomůže organizaci k zajištění shody s ČSN/ISO 27001:2013 o pořízování auditních záznamů, plnění požadavků GDPR či Zákona o kybernetické bezpečnosti. LOGmanager však není určen pouze pro oddělení bezpečnosti IT. Při vývoji LOGmanageru je kladen velký důraz na radikální jednoduchost užívání a jeho reálný přínos pro IT obecně. LOGmanager na jednom místě shromáždí provozní a diagnostická data ze všech důležitých systémů organizace. Operátor IT tak dostane možnost zjistit během několika sekund informace o provozních stavech a případných závadách, které by jinak musel hodiny komplikovaně vyhledávat v distribuovaných zdrojích. K tomu je i automaticky informován o sledovaných událostech a může tak předcházet kritickým IT nebo bezpečnostním incidentům.

PODPOROVANÁ ZAŘÍZENÍ

LOGmanager nativně podporuje více než 125 zdrojů ze všech oblastí IT, od bezpečnostních řešení, přes síť, virtualizace, operační systémy, databáze, až po cloud aplikace. Seznam zdrojů se každou aktualizací rozšiřuje. LOGmanager dále podporuje standardizované strukturované formáty logů, jako jsou CEF, LEEF, RFC5424 a JSON. Pro unikátní zdroje dat umožňuje rychlé a snadné vytvoření zákaznických parserů.

KLÍČOVÉ VLASTNOSTI

- Centrální úložiště logů, událostí a strojových dat organizace
- Sjednocení formátu zdrojových logů do lidsky srozumitelné formy
- Zpracování a vizualizace přijímaných dat v reálném čase
- Rychlé prohledávání dat bez nutnosti znalosti SQL jazyka
- SIEM funkce. Alerty na základě podmínek s limity a korelacemi
- Unikátní grafické konfigurační a programovací rozhraní
- Radikální jednoduchost a uživatelská přívětivost
- Snadné vytváření reportů a auditních zpráv za běhu
- Umožní snadnější splnění požadavku na shodu s regulacemi pro:

- GDPR
- Zákon o kybernetické bezpečnosti a návazné vyhlášky
- ČSN/ISO 27001:2013 pro pořizování auditních záznamů
- PCI DSS 3.2
- Bez licenčních omezení na množství zdrojů, výkon a uložená data
- Úsporu na licencích při budoucím rozšíření směrem k SIEM/UBA

Validace technického řešení s požadavky v uvedenými v ZD

Návrh, dodání a implementace nástroje pro centrální sběr, ukládání a správu logů s možností následné analýzy a řešení bezpečnostních událostí/incidentů z libovolných zdrojů (SEM/SIEM řešení). Pro účely případného bezpečnostního auditu musí dodané řešení uchovávat originály přijatých logů a pomáhat plnit požadavky bezpečnostních norem zadavatele i platné státní legislativy. Řešení musí sbírat provozní informace ze všech kritických prvků síťové infrastruktury, ukládat je na centrální úložiště a dlouhodobě je tam uchovávat tak, aby pověřený pracovník zadavatele měl kdykoliv snadný přístup k informacím o bezpečnostních incidentech, provozních stavech i případných závadách v prostředí své ICT sítě. Tyto informace musí být přístupné jak v reálném čase, tak nejméně rok zpětně. Systém musí být schopen vytvářet a odesílat hlášení o aktivitě jednotlivých prvků infrastruktury i uživatelů, dále musí dokázat generovat pravidelné i mimořádné auditní přehledy s požadovaným obsahem, aniž by operátor musel ovládat SQL příkazy – **ANO, nabízené řešení splňuje**

Dodavatel poskytne Objednateli po dobu trvání podpory všechny relevantní SW releases a verze SW nabízené výrobcem tak, aby dodané řešení vyhovovalo zadání zadavatele a fungovalo bez závad. Dodavatel se zároveň zavazuje informovat Objednatele o nových SW verzích a funkcích, které mohou rozšiřovat dodané řešení způsobem, který zadavatel shledá ve shodě s potřebami dalšího rozvoje dodaného řešení. Dodavatel se dále zavazuje získat potřebné SW produkty legálním způsobem za podmínek stanovených výrobcem zařízení – **ANO, veškeré podpory včetně nových release a rozvoje jsou v nabízeném řešení.**

Systém musí být snadno a plně obsluhovatelý stávajícím personálem zadavatele. Veškeré operace proto musejí probíhat prostřednictvím jednotného grafického rozhraní, které obsahuje předpřipravené reporty (např. změny v systémech provedené administrátory; seznam nově vytvořených účtů v MF ED v zadaném období; změny v přístupových právech pro určitého uživatele nebo k určité složce; monitoring privilegovaných účtů, sdílených účtů a konfiguračních změn; sledování souborových systémů atd.) Současně ale musí být možné vytvářet i vlastní reporty a pohledy na uložená data. Dodané zařízení musí sledovat chování uživatelů a dokázat automaticky upozorňovat na překračování pravidel na základě administrátorem zadaných limitů či korelací – **ANO, nabízené řešení splňuje**

Dodané zařízení by nemělo být jen jednotným úložištěm logů, ale mělo by disponovat pokročilými nástroji pro jejich správu, analýzu a generování upozornění. Systém musí být zabezpečen tak, aby k němu měly přístup pouze zadavatelem autorizované osoby, a to v určeném rozsahu. Ani autorizované osoby ale nesmějí mít možnost mazat nebo jakkoliv pozměňovat uložené logy. Centrální grafické rozhraní musí umožňovat operátorovi systému vytvářet vlastní uživatelsky definovaná pravidla standardizace logů, upozornění i korelace. Grafické rozhraní musí být snadno pochopitelné po krátkém zaškolení. Není přípustné, aby k výše uvedeným činnostem byla nutná účast výrobce, dodavatele nebo znalosti programování. Podrobné postupy včetně vzorových příkladů musí být uvedeny v dokumentaci – **ANO, nabízené řešení splňuje**

Řešení musí podporovat možnost zálohování konfigurace i uložených dat a jejich následnou obnovu. Objem logů, které budou do zařízení zasílány, není možné přesně určit. Proto musí systém podporovat jak pravidelné, tak i mimořádné zálohování dat na externí úložiště, ideálně využitím SMB protokolu. V souladu s "Bezpečnostním doporučením NCKB pro Administrátory 2.0" požadujeme, aby doba uložení logovaných událostí byla nejméně 18 měsíců. Data uložená v systému musí být možno prohlížet kdykoliv bez zjevných prodlev způsobených reimportem nebo dekomprimací dat a bez nutnosti konfiguračních změn – **ANO, nabízené řešení splňuje**

K dodanému zařízení i všem souvisejícím komponentám musí uchazeč poskytnout kompletní dokumentaci v českém jazyce včetně poznámek k vydání (release notes). Tato dokumentace musí být plně srovnatelná s aktuální originální (např. anglickou) verzí a dostatečně názorná, aby budoucí operátor systému podle ní zvládl provádět běžnou obsluhu a konfiguraci, aniž by potřeboval konzultovat výrobce či dodavatele. Centrální uživatelské rozhraní musí být uživatelsky přívětivé a umožňovat obsluhu systému bez nutnosti používání skriptů, maker, konfigurací v příkazové řádce nebo terminálu. V dokumentaci by mělo být mimo jiné názorně popsáno, jak konfigurovat běžné zdrojové systémy, aby spolupracovaly s dodaným zařízením – **ANO, nabízené řešení splňuje**

Zahrnuje-li nabízené řešení jakékoli licence, nesmí být jejich legální používání časově omezeno. Dodané zařízení musí být plně funkční i po skončení období placené podpory – **ANO, nabízené řešení není nijak časově omezeno, je plně funkční i po skončení placené podpory**

Zadavatel si vyhrazuje právo vyžádat si poskytnutí funkčního vzorku nabízeného zařízení kvůli ověření funkčních vlastností a poskytnutý vzorek otestovat ještě před ukončením výběrového řízení. Pokud zadavatel tohoto svého práva využije, zájemce je povinen dodat funkční vzorek do dvou týdnů od výzvy zadavatele. Zadavatel si dále vyhrazuje právo vyžádat si nejméně tři reference na zákazníky téhož řešení ze stejného oboru činnosti, spolu s kontakty na příslušné odpovědné osoby, za účelem zjištění zkušeností s nabízeným zařízením – **Společnost Caleum a.s. je připravena v rámci výběrového řízení dodat funkční vzorek a poskytnout požadované reference**

Zadavatel vyžaduje, aby v okamžiku podání nabídky nabízené řešení již disponovalo níže uvedenými funkcemi. Nesmí se tedy jednat o funkce pouze plánované, např. v budoucí verzi software - **Caleum a.s. potvrzuje, že nabízené řešení disponuje všemi funkcemi ke dni podání nabídky.**

Detailní technická specifikace

a. Obecné požadavky

a. Systém musí pracovat jako hardwarová appliance s jedním uceleným webovým rozhraním pro všechny administrátorské i operátorské činnosti. Nevyžadovat instalaci dalších systémů a aplikací, vyjma podpory sběru na pobočkách a agenta pro sběr Windows logů. Objednatel požaduje doložit katalogový list produktu (datasheet) podrobně popisující hardwarové i softwarové parametry nabízeného systému – **ANO splňuje, systém funguje jako 1 HW appliance s jedním webovým rozhraním. Datasheet nabízeného řešení LOGmanager je přiložen jako příloha nabídky LOGmanager_Datasheet.pdf**

b. Systém musí provádět zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware, viz níže uvedený seznam – **ANO, splňuje. Veškeré aplikace, OS, HW z příloženého seznamu jsou podporovány a na systému probíhá zpracování událostí z těchto systémů.**

c. Veškerá konfigurace systému se musí provádět v grafickém rozhraní jednotné uživatelské webové konzole. Systém poskytuje podporu pro vizuální programování pro všechny kroky zpracování strojových dat. Ve webové konzoli není povinná konfigurace za využití skriptů, maker nebo textových konfiguračních polí, do kterých se skripty/makra vkládají – **ANO, splňuje**

d. Systém musí pracovat jako hardwarová appliance s jedním uceleným webovým rozhraním pro všechny administrátorské i operátorské činnosti. Nevyžadovat instalaci dalších systémů a aplikací, vyjma podpory sběru na pobočkách a agenta pro sběr Windows logů. Objednatel požaduje doložit katalogový list produktu (datasheet) podrobně popisující hardwarové i softwarové parametry nabízeného systému – **ANO, systém funguje jako 1 HW appliance s jedním webovým rozhraním – datasheet přiložen jako příloha nabídky LOGmanager_Datasheet.pdf**

e. Systém musí provádět zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware, viz níže uvedený seznam - - **ANO, splňuje, veškeré systémy dle níže uvedeného seznamu jsou podporovány (viz odstavec b. Podpora sběru událostí)**

f. Veškerá konfigurace systému se musí provádět v grafickém rozhraní jednotné uživatelské webové konzole. Systém poskytuje podporu pro vizuální programování pro všechny kroky zpracování strojových dat. Ve webové konzoli není povinná konfigurace za využití skriptů, maker nebo textových konfiguračních polí, do kterých se skripty/makra vkládají – **ANO, splňuje**

g. Systém musí umožňovat snadné vyhledávání událostí a okamžité vytváření grafických reportů (ad hoc) bez nutnosti dodatečného programování nebo aplikování dotazů v SQL jazyce. Reportovací nástroj musí být integrální součástí navrhovaného systému a musí se obsluhovat v jednotném rozhraní nabízeného produktu. Objednatel vyžaduje předložit link nebo .pdf soubor popisující způsob vytváření reportů – **ANO, splňuje <https://doc.logmanager.cz/manual/3.6.2/cs/web/logs/reports.html>**

h. Systém musí provádět ucelenou vizualizaci logů, událostí a strojových dat (grafy událostí). Vizualizace musí být dynamická, tj. volbou v jednom grafu se ostatní příslušné grafy v pohledu na data upraví dle požadované volby automaticky – **ANO, splňuje**

i. Systém musí umožňovat snadno vytvářet grafické znázornění událostí v dashboardech nad všemi uloženými daty za libovolné časové období bez nutnosti nejprve modifikovat konfiguraci systému nebo parametrů uložených dat. Historická data v požadované délce retence uložená v systému je možné prohlédávat okamžitě bez časových prodlev opětovného importu nebo dekomprimace starších dat, prohlédávání dat nesmí vyžadovat manuální konfiguraci a zásahy uživatele – **ANO, splňuje**

- j. Systém musí provádět automatické doplňování reverzních DNS záznamů a GeoIP informací k událostem a u GeoIP jejich grafické znázornění na mapě bez nutnosti využívat služeb třetích stran či externí aplikace – **ANO, splňuje**
- k. Systém musí podporovat nativní získávání logů z Office365. Objednatel požaduje předložit link na dokumentaci popisující nastavení systému v jednotném grafickém rozhraní tak, aby získával logy z Office365 – **ANO, splňuje**, <https://doc.logmanager.cz/manual/3.6.2/cs/web/sources/o365.html>
- l. Systém musí být imunní vůči přetížení systému, nesmí dojít ke ztrátě logů. Všechny přijaté nezpracované logy/události musí být ukládány do vyrovnávací paměti. Při výraznějším plnění vyrovnávací paměti musí být administrátor systému automaticky informován. Velikost vyrovnávací paměti nesmí být nižší než 50 GB – **ANO, splňuje**
- m. Systém musí umožňovat unifikované vyhledávání napříč všemi typy dat a zařízeními dle normalizovaných polí (uživatelské jméno, zdrojová IP, značka/tag apod.) – **ANO, splňuje**
- n. Dodavatel musí předložit potvrzení vystavené autorizovanou osobou o shodě, že nabízený systém splňuje požadavky normy ČSN/ISO 27001:2013 na pořizování auditních záznamů. Toto potvrzení není možné nahradit certifikátem na společnost dodavatele (subdodavatele) nebo výrobce nabízeného systému. Nelze nahradit čestným prohlášením - – **ANO, splňuje - potvrzení následuje za touto kapitolou**
- o. Systém musí mít možnost uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování. Továrně dodané pohledy na data nesmí jít administrátorem systému nevratně modifikovat – **ANO, splňuje**
- p. Systém musí obsahovat reportovací nástroj s přednastavenými nejběžnějšími reporty a možností vlastních úprav a vytvoření nových pohledů. Pro vytváření nových pohledů na data není přípustné používat povinně SQL jazyk – **ANO, splňuje**
- q. Systém musí obsahovat předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění – **ANO, splňuje**
- r. Na základě pohledu na uložená data systém musí umožnit provést export dat ve strukturovaném formátu tak, jak jsou v továrně nastaveném nebo uživatelsky nastaveném pohledu data skutečně zobrazena – **ANO, splňuje**
- s. Konfigurační a systémové rozhraní a dokumentace k těmto rozhraním musí být identické v anglickém i v českém jazyce. Nepřipouští se omezená dokumentace v českém jazyce nebo zjednodušená dokumentace odkazující na další dokumentaci v anglickém jazyce, případně na dokumentaci třetích stran. Objednatel požaduje předložit link na online dokumentaci nebo připojit .pdf soubor aktuální kompletní dokumentace k ověření jednotlivých vlastností navrhovaného systému – **ANO, splňuje** <https://doc.logmanager.cz/manual/3.6.2/cs/index.html>
- t. Systém musí nabízet kapacitní i výkonovou škálovatelnost – **ANO, splňuje**
- u. Čistá kapacita úložného prostoru (kapacita diskového pole) dostupná pro uložená data nabízeného systému musí být minimálně 40TB – **ANO, splňuje**
- v. Objednatel požaduje, aby ze systému bylo možné vytáhnout libovolné dva disky, bez ztráty dat a vlivu na funkčnost řešení. Redundance disků nesmí ovlivňovat požadovanou kapacitu úložiště – **ANO, splňuje**
- w. Systém musí obsahovat monitoring stavu systému - alertování při překročení prahových hodnot nebo chybě systému, přeposlání upozornění pomocí SMTP nebo Syslog – **ANO, splňuje**
- x. Objednatel požaduje, aby systém obsahoval REST-API pro integraci s externím monitorovacím systémem (Zabbix, Nagios, MRTG a další) a umožňoval autorizovaný přístup ke strukturované databázi logů. Objednatel požaduje předložit vzorový návod na integraci s externím monitorovacím systémem- **ANO, splňuje viz.** <https://forum.logmanager.cz/> **How to integrate LOGmanager with Zabbix** či **How to collect events from NAGIOS and parse them**. Návod v .pdf přidáváme jako přílohu nabídky pod názvem dokumentu: **Napojení na Zabbix a další.pdf**
- y. Dodavatel doloží prohlášení výrobce o shodě s požadavky Vyhlášky 82/2018 Sb. „O bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)“ k Zákonu 181/2014 Sb. „O kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)“ – **Prohlášení je přiloženo na konci této kapitoly**

z. Systém musí obsahovat jednotnou centrální webovou konzoli s jednotným grafickým rozhraním pro přístup k logům, alertům, reportům a pro správu systému. Z této konzole se provádí veškerá konfigurace, správa i analýza logů. Není přípustné, aby navrhovaný systém měl více rozdílných konzolí od různých výrobců s rozdílným ovládáním. Objednatel požaduje předložit dokumentaci, ze které je zřejmé, jakým způsobem je realizována konfigurace v rámci jednotné konzole - **ANO, splňuje**

<https://doc.logmanager.cz/manual/3.6.2/cs/index.html>

<https://doc.logmanager.cz/manual/3.6.2/cs/web/logs/dashboards.html>

aa. Objednatel požaduje, aby systém umožňoval jednotné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem a jednotlivým ovládacím komponentám systému. Objednatel požaduje připojit odkaz na dokumentaci popisující vytváření uživatelských rolí **ANO, splňuje**:

Systémové skupiny: <https://doc.logmanager.cz/manual/3.6.2/cs/web/users/sysgroups.html>

Databázové skupiny: <https://doc.logmanager.cz/manual/3.6.2/cs/web/users/dbgroups.html>

bb. Dodaný systém musí obsahovat ucelené all-in-one řešení pro parsování a normalizaci přijatých událostí bez nutnosti dodatečné instalace externích aplikací nebo systémů. Jedinou přípustnou výjimkou je monitorování systémů Windows pomocí agentů – **ANO, splňuje**

cc. Systém musí podporovat ověřování uživatele systému na externím LDAP serveru. V případě výpadku externího LDAP systému musí podporovat ověření lokálního účtu. Systém automaticky zaznamenává uživatelská jména u akcí provedených konkrétním uživatelem – **ANO, splňuje**

b. Podpora sběru událostí

Systém musí nativně podporovat logy minimálně z následujících systémů: Amavis, Antivir AVG, Antivir Eset Remote administrator, Apache httpd, Apache Tomcat, ArcSight CEF (generický/standardizovaný formát), Brocade FC switches, Cisco ASA, Cisco Firepower, Cisco IOS, Cisco IronPort, Cisco ISE, Cisco SMB, Cisco UCS, Dell Force10, Dell iDrac (Server OoB management), Dell PowerConnect, Dropbear SSH (mostly Embedded Linux), Epacs, FlowMon, FreeRADIUS, HAProxy (structured rfc5425 logformat), ISC BIND, ISC DHCP, JSON (generický/standardizovaný formát), Kaspersky Endpoint Security, Kaspersky Security Center, Lenovo XClarity (Server OoB management), Linux Cron, Linux Freeradius, Linux Iptables, Linux Postfix, Microsoft Exchange log, Microsoft SharePoint, Microsoft SQL, Microsoft Windows DHCP log, Microsoft Windows DNS debug log, Microsoft Windows Firewall (optimized for performance), Microsoft Windows IIS/ftpserver, Microsoft Windows IIS/webserver, Mikrotik, MySQL, Nginx, Microfocus eDirectory, Office365, OpenSSH server, Oracle DB, PostgreSQL, Qradar LEEF (generický/standardizovaný formát), RFC5425 (generický/standardizovaný formát), Safetica DLP, Shorewall, Sophos, SpamAssasin, Squid (Web Proxy), Squid for Windows, Symantec Endpoint Protection Manager, Symantec Messaging Gateway, (brightmail), Synology NAS DSM, UBNT Rocket, UBNT UniFI, VMware, Windows - any logs from Event Viewer, Windows - any text log from file – **nabízené řešení LOGmanager nativně podporuje veškeré systémy uvedené v tomto odstavci**

c. Alerty

a. Systém musí být schopen na základě uživatelsky zadaných podmínek splněných v přijatých datech vygenerovat alert – **ANO, splňuje**

b. Text emailu vygenerovaného alertem musí být uživatelsky definovatelný s proměnnými, které jsou vyplněny z přijaté rozparované události – **ANO, splňuje**

c. Systém musí obsahovat výrobcem předpřipravené sety/vzory alertů a korelací – **ANO, splňuje**

d. Systém musí provádět konfigurace alertů a korelací pomocí vizuálního programovacího jazyka. Vizuální programovací jazyk není prezentován čistě textově, ale textově-grafickou formou, která vizualizuje aplikační logiku vytvářeného alertu. Konfigurace alertů musí umožňovat okamžitou kontrolu funkčnosti výstupu alertu nebo korelace vložení příslušné testovací zprávy, včetně zobrazení upozornění na případné uživatelské chyby. Objednatel požaduje dodat odkaz na dokumentaci, jakým způsobem realizujete konfiguraci a testování alertů a korelací - **ANO, splňuje** <https://doc.logmanager.cz/manual/3.6.2/cs/web/logs/alerts.html>

e. Jako výstupní pravidlo Alertu musí systém umět odeslat událost, která alert vyvolala, na externí systém minimálně prostřednictvím SMTP nebo Syslogu přes TCP protokol. U Syslog protokolu požadujeme možnost definice formátu odesílaných dat pro snazší integraci se systémy třetích stran. Objednatel požaduje doložit odkazem na dokumentaci, jakým způsobem se zpráva, která vyvolala spuštění alertu, odesílá na externí systém a jak se definuje formát odesílání dat – **ANO, splňuje**

<https://doc.logmanager.cz/manual/3.6.2/cs/web/logs/syslogOutput.html>

f. Objednatel požaduje, aby Systém umožňoval v alertech využít značky (příklad: pošli alert jen v případě, že se událost stala na kritickém serveru a je označen názvem lokality) – **ANO, splňuje**

g. Systém musí podporovat základní funkce SIEM - funkce pro korelace událostí a upozornění s hraničními limity. Definice korelačních pravidel je prováděna pomocí vizuálního programovacího jazyka a musí obsahovat možnost vložení testovací zprávy a výsledku testu o provedené akci – **ANO, splňuje**

d. Sběr událostí z Microsoft systémů

a. Události z Microsoft systémů musí být vyčítány pomocí agenta instalovaného přímo v koncových systémech. Windows agent musí současně podporovat jak monitoring interních windows logů, tak monitoring textových souborových logů. Objednatel požaduje doložit kompletní dokumentaci a poznámky k vydání (release notes) k agentu pro sběr událostí z prostředí Microsoft - **Ano, splňuje. Release notes jsou přiloženy v rámci podané nabídky jako dokument LOGmanager-release-notes-3.6.2_CZ.pdf**

b. Agent musí zajišťovat sběr nemodifikovaných událostí a detailní zpracování auditních informací – **ANO, splňuje**

c. Agent musí podporovat nastavení filtrace odesílaných událostí pomocí centrální správčovské konzole – **ANO, splňuje**

d. Filtrace odesílaných událostí agentem se musí konfigurovat pomocí vizuálního programovacího jazyka z centrální správčovské konzole systému. Logy nastavené k filtraci jsou filtrovány na straně windows agenta a nejsou nijak odesílány po síti. Vizuální programovací jazyk není prezentován textově, ale textově-grafickou formou, která vizualizuje aplikační logiku vytvářeného alertu. Filtry musejí umožňovat okamžitě testovat jejich účinnost a zobrazit kolik z uložených dat zvolený filtr zasáhne a kolik logů by případně filtroval minimálně za posledních 24 hodin. Objednatel požaduje doložit odkazem na dokumentaci, jakým způsobem se vytváří a přiřazují filtry pro windows agenty pro sběr logů a jakým způsobem se testuje účinnost filtru – **ANO, splňuje**

<https://doc.logmanager.cz/manual/3.6.2/cs/web/sources/windowsfilters.html#pridani-noveho-filtru>

e. Windows agent nesmí vyžadovat administrátorské zásahy na koncovém systému – je centrálně spravovaný a jeho konfigurace musí být kompletně realizována v grafickém rozhraní systému bez využití skriptů nebo maker. Konfigurace musí být automaticky distribuována přímo z centrální konzole systému. Správa a aktualizace Windows agenta se neprovádí z Group Policy. Objednatel požaduje doložit odkazem na dokumentaci, jakým způsobem se centrálně z grafického rozhraní spravují Windows agenti včetně všech možností nastavení – **ANO, splňuje - https://doc.logmanager.cz/manual/3.6.2/cs/web/sources/windows.html**

f. Agent musí automaticky překládat zástupné kódy status ve zprávách na text (např. Logon Type 2 = Interactive, Logon Type 3 = Network, atd.) – **ANO, splňuje**

g. Windows agent musí obsahovat buffer pro případ ztráty spojení mezi koncovým systémem a centrálním úložištěm logů – **ANO, splňuje**

h. Komunikace Windows agenta a centrálního systému musí být šifrovaná – **ANO, splňuje**

i. Windows agent musí podporovat sběr nejen ze základních systémových logů (Aplikace, Zabezpečení, Instalace, Systém), ale je možné z centrální konzole v grafickém rozhraní nastavit i sběr všech ostatních logů ve složce Protokoly aplikací a služeb. Dále musí Windows agent podporovat centralizované nastavení z administrátorské konzole systému pro sběr textových logů včetně možnosti výběru jejich formátu. Objednatel požaduje doložit odkazem na dokumentaci, jakým způsobem se nastavují parametry sběru logů globálně a jakým způsobem u konkrétního agenta. – **ANO, splňuje**

Dokumentace Windows Agentů globálně:

<https://doc.logmanager.cz/manual/3.4.0/cs/web/sources/windowssettings.html>

Dokumentace nastavení vybraného Windows Agenta:

<https://doc.logmanager.cz/manual/3.4.0/cs/web/sources/windows.html#editace-klientske-stanice>

j. Windows agent musí automaticky doplňovat ke všem odesílaným událostem jejich textový popis tak, jak je zobrazen v Prohlížeči událostí (Event Viewer) na koncovém systému – **ANO, splňuje**

k. Počet instalací Windows agenta nesmí být licenčně a časově omezen – **ANO, splňuje - bez licenčního a časového omezení**

e. Podpora pro sběr událostí z jiných míst

a. Systém musí obsahovat centrálně spravované řešení, které sbírá události na pobočkách a umožní jejich odeslání po saturované lince bez ztráty dat. Objednatel požaduje doložit odkazem na dokumentaci, jakým způsobem realizujete sběr událostí z poboček – **ANO, splňuje**

<https://doc.logmanager.cz/manual/3.6.2/cs/forwarder.html>

b. Systém musí podporovat centralizovanou správu pro sběr událostí přímo z centrálního úložiště dat včetně dokumentace požadavků na virtualizaci a komunikační matici pro šifrovaný přenos dat – **ANO, splňuje**

c. Řešení musí být schopno automaticky navázat spojení s centrálním úložištěm dat a přenášená data šifrovat. V případě výpadku spojení mezi pobočkou a centrálou musí spojení automaticky obnovit – **ANO, splňuje**

d. Řešení musí komunikovat po definovaném IP protokolu, aby mohla být centrálně nastavena kvalita služby (QoS) pro přenos událostí – **ANO, splňuje**

e. Řešení musí poskytovat kapacitu vyrovnávací paměti pro minimálně 100GB událostí, které na pobočce mohou vzniknout během výpadku spojení mezi pobočkou a datovým centrem – **ANO, splňuje**

f. Řešení pro sběr dat z poboček musí mít výkon minimálně 5 tisíc událostí/s, a to i v trvalé zátěži – **ANO, splňuje**

g. Řešení musí poskytnout podporu pro sběr událostí na identických UDP i TCP portech jako hlavní dodaný systém – **ANO, splňuje**

h. Řešení musí být k dispozici jako fyzický systém nebo jako virtuální systém pro VMware ESXi a Hyper-V – **ANO, splňuje**

i. Řešení musí být schopno komunikovat z pobočky na centrálu i přes vícenásobný překlad adres (NAT) – **ANO, splňuje**

f. SW parametry systému

a. Systém musí fungovat formou HW appliance (všechny části systému je možné nastavit v centrální správčovské konzoli, například není nutné editovat žádné konfigurační soubory, skripty nebo makra) – **ANO, splňuje**

b. Aktualizace systému musí být distribuovány v jednotném balíku a jejich instalace je prováděna uživatelsky přes centrální webovou správčovskou konzoli. Všechny aktualizace musí být prováděny z webového prostředí bez potřeby asistence dodavatele/výrobce dodávaného systému. Požadujeme předložení posledních 4 poznámek k novému vydání (release notes) pro kontrolu parametrů navrhovaného systému **ANO, splňuje – V release notes, které jsou součástí podané nabídky jako samostatný dokument LOGmanager-release-notes-3.6.2_CZ.pdf, jsou uvedeny 4 poznámky k novému vydání**

c. Systém musí podporovat downgrade v jednom kroku, pro případ problémů s novou verzí systému po upgrade. Není přípustný downgrade pouze za součinnosti výrobce. Popište podrobně způsob realizace downgrade - **ANO, splňuje**

Downgrade je možné spustit volbou verze software, a to během bootu zařízení z konzole appliance. LOGmanager zachovává poslední 4 verze operačního systému automaticky pro možný downgrade. Během downgrade nedojde k narušení konzistence uložených dat.

d. Systém musí umožňovat průměrný trvalý příjem min. 5 tisíc událostí/s, s možností navýšení na minimálně 6 tis. událostí/s prostřednictvím licence nebo rozšíření hardware. Výkon musí odpovídat pro požadované množství událostí s průměrnou délkou 600Byte - **ANO, splňuje**

e. Systém musí umožňovat špičkový příjem minimálně 10 tisíc událostí/s po dobu nejméně 10 minut, v případě vyššího počtu událostí, než je průměrný trvalý příjem, je systém uloží do bufferu a zpracuje později - **ANO, splňuje**

f. Systém musí mít licenčně neomezený počet zařízení pro příjem zasílaných událostí. Licenčně neomezený počet událostí v GB za den nebo licence na minimálně 300GB uložených událostí za den. Integrovaná databáze musí mít čistou velikost nejméně 40TB a nad to musí podporovat kompresi ukládaných dat - **ANO, splňuje. Integrovaná DB má čistou kapacitu 40 TB včetně podpory komprese.**

g. Systém musí obsahovat uživatelskou konfiguraci vlastních parserů pomocí vizuálního programovacího jazyka v centrální správcovské webové konzoli. Vizuální programovací jazyk musí uživateli umožnit psát vlastní parsery bez nutnosti znalosti programování (např. NodeRED, Microsoft VPL, Blockly apod). Vizuální programovací jazyk není prezentován textově, ale graficky formou schémat-symbolů, které reprezentují aplikační logiku a kontrolují syntaxi - **ANO, splňuje**

h. Konfigurace uživatelských parserů musí umožňovat automatické doplňování DNS reverzních záznamů, GeoIP informace a identifikace výrobce zařízení podle MAC adresy - **ANO, splňuje**

i. Systém musí podporovat doplňování zpráv o statické informace z textových tabulek. (Například k uživatelskému jménu doplnit informaci o jeho emailu, členství v AD skupinách a podobně). Pro automatickou aktualizaci takto uložených doplňujících informací musejí být tyto textové tabulky naplnitelné pomocí REST API nabízeného systému a modifikovatelné přes webové rozhraní - **ANO, splňuje**

j. Systém musí obsahovat možnost on-line ladění uživatelsky definovaných parserů - při jejich vytváření je možné vložit skupinu testovacích zpráv, při změně je okamžitě zobrazena výsledná podoba rozparovaných dat a případná chybová hlášení s upozorněním na chybná místa vytvářeného parseru. Pro snadnější vytváření parserů požadujeme mít možnost vložení minimálně 20 testovacích zpráv současně. Objednatel požaduje doložit odkazem na dokumentaci, ze které je zřejmé, jakým způsobem se vkládají testovací zprávy během psaní nového uživatelského parseru a jakým způsobem je prezentován výstup testu - **ANO, splňuje**

https://doc.logmanager.cz/manual/3.6.2/cs/web/parser/parsing_rule.html#pridani-parsovacihopravidla

k. Systém musí mít možnost v centrální správcovské konzoli přidávat k jednotlivým zdrojům dat, aplikacím, zařízením nebo IP subnetům tzv. značky, označující například umístění zařízení, typ zařízení, kritičnost zařízení apod. Systém obsahuje předdefinované značky, které automaticky přidává k přijímaným zprávám. Příklady značek: konfigurační změna, úspěšné ověření uživatele, neúspěšné ověření uživatele, zpráva přišla z windows, zpráva byla vygenerována firewallem atd - **ANO, splňuje**

l. Systém musí mít možnost v centrální správcovské konzoli při definici vlastního parseru přidávat značky pro typy událostí (login, logout apod.) - **ANO, splňuje**

m. Systém musí mít možnost všechny přidávané značky ukládat s každou přijatou událostí, na základě značky je možné filtrovat data nebo omezovat oprávnění uživatelů systému k jednotlivým událostem - **ANO, splňuje**

n. Pro budoucí nasazení ve vysoké dostupnosti je vyžadována podpora sestavení v clusteru – požadujeme podporu minimálně 2 nodů. Nastavení clusteru se musí kompletně realizovat v grafickém rozhraní správcovské konzole v jednom kroku, není přípustné konfigurovat sestavení scripty, makry nebo úpravou textové konfigurace systému a pomocí ručních restartů služeb. Systém ve vysoké dostupnosti musí přehledně informovat o stavu clusteru a procesu synchronizace databází. Dokumentace k realizaci vysoké dostupnosti musí být kompletní a popisovat všechny kroky sestavování a obnovení v případě výpadku komponenty clusteru. Objednatel požaduje doložit odkazem na dokumentaci, jakým způsobem se cluster vytváří a jakým způsobem se provádí obnovení po možném výpadku jednotlivých zúčastněných komponent - **ANO, splňuje**

<https://doc.logmanager.cz/manual/3.6.2/cs/web/system/cluster.html>

o. Objednatel vyžaduje, aby se budoucí dvounodový cluster choval jako 1 celek. V případě využití dvou nodů v clusteru se zrychluje vyhledávání a jsou automaticky prohledávána všechna data na všech zařízeních v clusteru- **ANO, splňuje**

p. V případě rozšíření systému na cluster (2 nody) musejí zařízení odesílající události odesílat pouze na jednu virtuální adresu (řízenou aktivním prvkem počítačové sítě) a zároveň cluster musí zajišťovat synchronizaci konfigurace a událostí mezi nody - **ANO, splňuje**

q. Řešení musí umožňovat rozšíření mezipaměti diskového subsystému o SSD nebo NVRAM typu o kapacitě minimálně 3TB - **ANO, splňuje**

r. Systém musí umožňovat export dat ve formátu vhodném pro další strojové zpracování bez dodatečných omezení na časové období, množství nebo obsah exportovaných dat. Během exportu je možné označit pouze vybraná pole, která mají být do exportu zahrnuta - **ANO, splňuje**

s. Systém musí podporovat zálohování nebo obnovení konfigurace v jednom kroku a jednom souboru pro celý systém. Objednatel požaduje doložit odkazem na dokumentaci, jakým způsobem se provádí zálohování a obnova konfigurace systému - **ANO, splňuje**

<https://doc.logmanager.cz/manual/3.6.2/cs/web/system/backup.html#zaloha-obnova-konfigurace>

t. Podpora zálohování dat na externí systém. Je požadováno plánované i ad-hoc zálohování. Zálohy dat musejí být vhodně kompresovány. Systém umožňuje obnovit data ze záloh a během obnovy je automaticky znova indexovat tak, aby bylo možné v datech obnovených ze záloh pracovat shodně jako s aktuálním obsahem databáze. Zálohování musí jít kompletně nastavit v uživatelském rozhraní systému, nepřípouští se využívání skriptů, maker nebo textových konfiguračních souborů. Objednatel požaduje doložit odkazem na dokumentaci, jakým způsobem se realizuje zálohování a obnova záloh - **ANO, splňuje**

<https://doc.logmanager.cz/manual/3.6.2/cs/web/system/backup.html>

g. Minimální HW parametry na požadovaných systém

a. Jedna hardwarová appliance o velikosti max. 2U, včetně ramena pro kabelový management umožňujícího vysunutí zapnutého systému z racku pro servisní účely - **ANO, splňuje**

b. HW appliance musí obsahovat veškeré potřebné komponenty (CPU, RAM, diskový prostor) pro svoji činnost a je nezávislá na dalších systémech - **ANO, splňuje**

c. 2 procesory, min. 12 jader každý, s podporou HyperThreadingu - **ANO, splňuje**

d. Min. 128GB DDR-4 a možnost rozšíření o NVMe paměťové pole pro zpracování dat v čase blízkém reálnému (Near Real-Time) - **ANO, splňuje**

e. Minimálně 40TB pro integrovanou databázi podporovanou HW akceleračním SAS RAID řadičem s read-write cache min. 8GB. Řadič diskového pole musí obsahovat zálohovací baterii nebo být vybaven flash pamětí - **ANO, splňuje – 40 TB databáze včetně akceleračního RAID řadiče(SAS)**

f. Z výkonových důvodů požadujeme, aby v systému bylo minimálně 12 ks stejných RAID edition disků určených pro použití v datacentrech, o rychlosti minimálně 7200 otáček/m - **ANO, splňuje**

g. Minimálně 4x 1Gbit LAN porty + 1x dedikovaný 1Gbit port pro management HW. Konfigurace všech parametrů síťového rozhraní včetně link agregace dle LACP (802.3ad) ve webovém rozhraní systému a příslušný popis v dokumentaci - **ANO, splňuje**

h. Větráky v systému musí být vyměnitelné za provozu a redundantní - **ANO, splňuje**

i. 2x napájecí zdroje s redundancí napájení 1+1 - **ANO, splňuje**

j. Virtuální KVM (tj. převzetí textové i grafické konzole serveru a zajištění přenosu povelů z klávesnice a myši vzdáleného počítače) - **ANO, splňuje**

k. Systém pro vzdálenou správu serveru včetně potřebné licence, pokud je třeba (obdoba HP iLO, Dell iDRAC apod) - **ANO, splňuje**

h. SW Podpora, záruka na hardware, vysoká dostupnost

a. Požadujeme volitelnou podporu pro nasazení ve vysoké dostupnosti - **ANO, splňuje – volitelná podpora pro HA je možná**

b. HW - Požadovaná min. 5letá servisní podpora na hardware appliance s opravou v místě instalace serveru a s garantovanou odezvou následující pracovní den od nahlášení případné závady - **ANO, splňuje**

c. SW - Podpora výrobce na aktualizaci systému a parserů na 3 roky. Podpora musí obsahovat aktualizaci SW minimálně 4x ročně, opravy chyb a telefonickou a emailovou podporu s diagnostikou vzdáleným přístupem **ANO, splňuje**

OVĚŘENÍ FUNKČNÍCH VLASTNOSTÍ

Caleum a.s. potvrzuje, že v případě výzvy Zadavatele provede ověření funkčních vlastností tak, jak je uvedeno v kapitole níže:

Vyzve-li zadavatel uchazeče k poskytnutí funkčního vzorku pro testování a ověření požadovaných funkčních vlastností, je uchazeč povinen doručit testovací vzorek na zadavatelem určené místo do dvou týdnů od doručení výzvy. Vyzvaný uchazeč poskytne testovací zařízení včetně české dokumentace bezplatně a na dobu minimálně 10 pracovních dnů. Zadavatel otestuje s použitím poskytnuté dokumentace na dodaném testovacím zařízení níže uvedené činnosti a následně vyhotoví záznam o průběhu a výsledcích testování:

- Základní nastavení a konfigurace systému pro efektivní využití v prostředí zadavatele, včetně vytvoření několika uživatelů s různými oprávněními k systému a datům;
- Nastavení několika vybraných zdrojových systémů, aby posílaly logy a události do dodaného zařízení, a otestování těchto činností:
 - nastavení klasifikace zdrojů
 - nastavení značek (tagů)
 - filtrování událostí
 - modifikace parsování existujícího zdroje v grafickém rozhraní nástroje;
- Konfigurace vybraných Microsoft Windows systémů, aby posílaly logy do testovaného systému;
- Ověření funkčních a výkonových parametrů agenta pro sběr událostí z vybraného prostředí, dle požadavků ze seznamu podporovaných systémů
- Vytvoření a uložení vlastního dashboardu a reportu, nastavení pravidelného odesílání reportů mailem vybraným pracovníkům zadavatele;
- Ověření způsobu, jakým se v jednotném grafickém rozhraní vytváří klasifikace a filtrování vstupních dat;
- Vytvoření, konfigurace a odladění jednoduchého uživatelsky definovaného parseru
- Nastavení značkování událostí, vytváření upozornění s limity nebo korelacemi podle požadavků zadavatele (příklad 1: pošli alert jen v případě, že se událost stala na skupině síťových přepínačů 10krát během 10 minut. Příklad 2: pošli alert v případě, že uživatel za posledních 10 minut smazal na všech serverech více než 10 souborů, bez započtení smazání dočasných souborů);
- Odeslání události, která vyvolala alert, na externí syslog server přes TCP protokol;
- Simulace úplného selhání systému a následná oprava ze záloh v těchto krocích:
 - Záloha konfigurace a dat na externí systém
 - Uvedení systému do továrního nastavení
 - Obnova konfigurace a všech dat z vytvořených záloh
 - Kontrola úplnosti obnovené konfigurace a dat ze záloh;

- Upgrade a downgrade softwaru systému v centrálním grafickém rozhraní a provedení kontroly, zda v případě downgrade nedošlo ke ztrátě dat. Kontrola souladu změn funkčních vlastností po upgrade softwaru s popisem v poznámkách k danému vydání softwaru (release notes k jednotlivým testovaným verzím softwaru);
- Kontrola kompletnosti české dokumentace systému;
- Ověření požadovaných parametrů a vlastností dodaného funkčního vzorku systému dle podmínek uvedených v této zadávací dokumentaci.

Ověření funkčních vlastností nabízeného řešení provede zadavatel podle dokumentace poskytnuté uchazečem. V případě nejasností vyzve zadavatel zástupce dodavatele/uchazeče, který mu poskytne potřebnou součinnost, a to nejpozději do 3 pracovních dnů po doručení výzvy uchazeči. Testy budou prováděny v prostředí zadavatele. Po ukončení testování bude funkční vzorek uchazeči vrácen (uchazeč si vyzvedne vzorek na vlastní náklady v místě testování).

Zadavatel zakončí testování vyhotovením zápisu. Pokud testovaný systém neprojde úspěšným ověřením funkčních vlastností, neuzavře zadavatel s takovým uchazečem smlouvu, a vyzve k dodání testovacího vzorku toho uchazeče, který se v hodnocení nabídek umístil jako další v pořadí.

ROZSAH IMPLEMENTAČNÍCH PRACÍ

Caleum a.s. potvrzuje, že v rámci implementace budou provedeny následující práce:

Předmětem je instalace HW a SW centrálního úložiště pro sběr a analýzu logů a událostí ze systémů, serverů a aplikací zadavatele. Dále pak implementace a konfigurace systému do prostředí Objednatele, zaškolení zaměstnanců Objednatele v provozování Systému, které bude mít zhruba tuto osnovu:

- a) instalace, konfigurace a správa systému včetně log databáze,
- b) ovládní GUI, definice alertů, reportingu, analýzy logů,
- c) tvorby vlastních parserů pomocí vizuálního programovacího jazyka
- d) konzultace k používání systému dle potřeb Objednatele

A následně provozní dokumentace obsahující popis instalovaného řešení a mapu toku logů z jednotlivých zdrojů do centrálního úložiště, specifikaci nastavení alertů reportů a transformace logů do požadované formy.