

Příloha č. 1 - Specifikace předmětu plnění (Část B)

Technická specifikace dodávaného zařízení – LOGmanageru (včetně technické podpory a záruky)

Zadavatel vyžaduje, aby nabízené řešení mělo níže požadované funkce již v době podání nabídky, nikoliv aby se jednalo o budoucí funkce plánovaných verzí software pro nabízené řešení. Dodavatel (uchazeč) vyplní nabízenou konfiguraci tak, aby splňovala minimální požadavky zadavatele.

	Popis - Řešení SEM/SIEM do 5000 událostí/s s minimálně 40TB velikostí databáze	Logmanager -XL s kapacitu 109 TB a 10000 EPS, špičkově 20000 EPS
	Obecné požadavky na systém pro centralizovanou správu logů, událostí a strojových dat	Technická specifikace nabízeného řešení
1	Systém pracuje jako hardwarová appliance s jedním uceleným webovým rozhraním pro všechny administrátorské i operátorské činnosti. Nevyžaduje instalaci dalších systémů a aplikací, vyjma podpory sběru na pobočkách a agenta pro sběr Windows logů. Doložte katalogový list produktu (datasheet) podrobně popisující hardwarové i softwarové parametry nabízeného systému.	Ano, systém pracuje jako hardwarová appliance s jedním uceleným webovým rozhraním pro všechny administrátorské i operátorské činnosti. Nevyžaduje instalaci dalších systémů a aplikací, vyjma podpory sběru na pobočkách a agenta pro sběr Windows logů. Datasheet naleznete zde: https://logmanager.com/cs/podpora#documents-for-download
2	Systém provádí zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware.	Ano, systém provádí zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware.
3	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 se nepřipouští konfigurace za využití skriptů, maker nebo textových konfiguračních polí, do kterých se složité textové skripty/makra vkládají.	Ano, veškerá konfigurace systému se provádí v grafickém rozhraní jednotné uživatelské webové konzole. Systém poskytuje podporu pro vizuální programování pro všechny kroky zpracování strojových dat. Ve webové konzoli se nekonfiguruje za využití skriptů, maker nebo textových konfiguračních polí, do kterých se složité textové skripty/makra vkládají.
4	Systém umožňuje dopsání parserů pro výše neuvedená zařízení uživatelem bez nutnosti spolupráce s výrobcem nebo dodavatelem (vč. subdodavatelů) nabízeného systému – Uživatelsky definované parsery. Dokumentace musí obsahovat přehledný návod na vytváření zákaznických parserů a systém musí obsahovat možnost testování a ladění zákaznických parserů v jednotném ovládacím grafickém webovém rozhraní viz bod č. 1. Vytváření a testování parserů nesmí mít vliv na provoz systému. Pro psaní parserů nesmí být použito textové psaní programového kódu ale tzv. vizuální programování, které automaticky opravuje uživatele a upozorňuje ho na chyby. Požadujeme předložit příslušnou dokumentaci k vytváření parserů a testování jejich funkčnosti.	Ano, Logmanager umožňuje dopsání parserů pro výše neuvedená zařízení uživatelem bez nutnosti spolupráce s výrobcem nebo dodavatelem (vč. subdodavatelů) nabízeného systému - uživatelsky definované parsery. Dokumentace obsahuje přehledný návod na vytváření zákaznických parserů a systém obsahuje možnost testování a ladění zákaznických parserů v jednotném ovládacím grafickém webovém rozhraní viz bod č. 1. Vytváření a testování parserů nemá vliv na provoz systému. Pro psaní parserů není použito textové psaní programového kódu, ale tzv. vizuální programování, které automaticky opravuje uživatele a upozorňuje ho na chyby. Dokumentace zde: https://doc.logmanager.com/latest/cz/web-interface/parser/parsers/
5	Systém umožňuje v grafickém rozhraní vizuálního programovacího jazyka snadno provádět třídění a značkování vstupních dat pro jejich další zpracování. Nepřipouští se nastavování třídění vstupních dat ve formě skriptu/makra zobrazeného v textovém okně. Předložte příslušný odkaz na dokumentaci popisující funkčnost třídění vstupních dat.	Ano, Logmanager umožňuje v grafickém rozhraní vizuálního programovacího jazyka snadno provádět třídění a značkování vstupních dat pro jejich další zpracování. Nepřipouští se nastavování třídění vstupních dat ve formě skriptu/makra zobrazeného v textovém okně. Dokumentace zde: https://doc.logmanager.com/latest/cz/web-interface/parser/classifiers/

6	Systém přijímá a zpracovává logy, události a další strojově generovaná data prostřednictvím minimálně následujících protokolů: SYSLOG (dle RFC3164, RFC5424, RFC5425) a RELP. Systém musí umožňovat příjem logů i na rozsahu alespoň 50 UDP a TCP portů pro zjednodušené třídění vstupních zpráv. Dále požadujeme podporu sběru strojových dat z databází s nastavením v grafickém menu systému minimálně pro databáze MSSQL, MySQL, Oracle a PostgreSQL a to bez nutnosti instalovat na databázový server doplňkový software nebo agenta. Předložte detailní komunikační matici nabízeného systému a dokumentaci k nastavení sběru z databází v grafickém rozhraní systému.	Ano, Logmanager přijímá a zpracovává logy, události a další strojově generovaná data prostřednictvím minimálně následujících protokolů: SYSLOG (dle RFC3164, RFC5424, RFC5425) a RELP. Systém umožňuje příjem logů i na rozsahu alespoň 50 UDP a TCP portů pro zjednodušené třídění vstupních zpráv. Dále Logmanager nabízí podporu sběru strojových dat z databází s nastavením v grafickém menu systému minimálně pro databáze MSSQL, MySQL, Oracle a PostgreSQL a to bez nutnosti instalovat na databázový server doplňkový software nebo agenta. U sběru dat z databází umí nastavit interval čtení. Komunikace Logmanageru zde: https://doc.logmanager.com/latest/cz/additional-informations/communication-of-logmanager
7	Přijaté logy systém standardizuje do jednotného formátu a logy jsou normalizovány (rozdělovány) do příslušných polí dle jejich typu. Zároveň systém uchovává i originální verzi zpráv. Integrované parsery systému automaticky přidávají ke zprávám, kterých se to týká, meta informace o jaký druh zprávy se jedná, minimálně požadujeme rozlišení těchto druhů zpráv: úspěšné přihlášení, neúspěšné přihlášení, odhlášení, konfigurační změna, značka/tag. Tyto meta informace musí být možné přidávat i v uživatelsky definovaných parserech.	Ano, přijaté logy systém standardizuje do jednotného formátu a logy jsou normalizovány (rozdělovány) do příslušných polí dle jejich typu. Zároveň systém uchovává i originální verzi zpráv. Integrované parsery systému automaticky přidávají ke zprávám, kterých se to týká, meta informace, o jaký druh zprávy se jedná, minimální rozlišení těchto druhů zpráv je: úspěšné přihlášení, neúspěšné přihlášení, odhlášení, konfigurační změna, značka/tag. Tyto meta informace je možné přidávat i v uživatelsky definovaných parserech.
8	Hodnoty jednotlivých parsovaných polí je možné v definici parseru přetypovat a standardizovat alespoň na tyto základní druhy: číslo, IP adresa, MAC adresa, URL. Nad uloženými čísly je pak možné při prohledávání dat provádět matematické operace (součty všech hodnot, průměry, nejmenší/největší hodnota apod.).	Ano, hodnoty jednotlivých parsovaných polí je možné v definici parseru přetypovat a standardizovat alespoň na tyto základní druhy: číslo, IP adresa, MAC adresa, URL. Nad uloženými čísly je pak možné při prohledávání dat provádět matematické operace (součty všech hodnot, průměry, nejmenší/největší hodnota apod.).
9	Systém zachovává původní informaci ze zdroje logu o časové značce události, ale nedůvěřuje jí a vytváří vlastní důvěryhodné časové razítko ke každému logu, které vzniká v okamžiku přijetí logu systémem a kterým se systém defaultně řídí.	Ano, Logmanager zachovává původní informaci ze zdroje logu o časové značce události, ale nedůvěřuje jí a vytváří vlastní důvěryhodné časové razítko ke každému logu, které vzniká v okamžiku přijetí logu systémem a kterým se systém defaultně řídí.
10	Všechna pole a položky přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem.	Ano, všechna pole a položky přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem.
11	Možnost sběru událostí minimálně ve formátech RAW, Syslog RFC5424, CEF, LEEF, JSON RFC8259.	Ano, Logmanager podporuje sběr událostí minimálně ve formátech RAW, Syslog RFC5424, CEF, LEEF, JSON RFC8259.
12	Systém nesmí v žádném případě umožnit mazání nebo modifikování již uložených logů v rámci požadované retence. A to ani libovolnou konfigurační změnou - administrátorovi s nejvyššími oprávněními k navrhovanému systému. Každý zpracovaný log musí mít dohledatelný unikátní identifikátor, který umožní jeho jednoznačnou identifikaci.	Ano, Logmanager nikdy neumožňuje mazání nebo modifikování již uložených logů v rámci požadované retence. A to ani libovolnou konfigurační změnou – administrátorovi s nejvyššími oprávněními k navrhovanému systému. Každý zpracovaný log má dohledatelný unikátní identifikátor, který umožní jeho jednoznačnou identifikaci.
13	Systém musí umožňovat konfiguraci filtrace nerelevantních událostí v grafickém rozhraní vizuálního programovacího jazyka. Pro psaní filtrace nesmí být použito textové psaní programového kódu ale tzv. vizuální programování, které automaticky opravuje uživatele a upozorňuje ho na chyby. Předložte odkaz na dokumentaci popisující způsob filtrování nerelevantních událostí.	Ano, Logmanager umožňuje konfiguraci filtrace nerelevantních událostí v grafickém rozhraní vizuálního programovacího jazyka. Pro psaní filtrace není použito textové psaní programového kódu, ale tzv. vizuální programování, které automaticky opravuje uživatele a upozorňuje ho na chyby. Odkaz na klasifikaci zde: https://doc.logmanager.com/latest/cz/web-interface/parser/classifiers/
14	Systém provádí konsolidaci logů na interním storage logovacího systému.	Ano, Logmanager provádí konsolidaci logů na interním storage logovacího systému.
15	Systém umožňuje 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. Předložte link nebo pdf popisující způsob vytváření reportů.	Ano, Logmanager umožňuje snadné vyhledávání událostí a okamžité vytváření grafických reportů (ad hoc) bez nutnosti dodatečného programování nebo aplikování dotazů v SQL jazyce. Reportovací nástroj je integrální součástí navrhovaného systému a obsluhuje se v jednotném rozhraní nabízeného produktu. Dokumentace zde: https://doc.logmanager.com/latest/web-interface/logs/reports/

16	Systém provádí 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, Logmanager provádí ucelenou vizualizaci logů, událostí a strojových dat (grafy událostí). Vizualizace je dynamická, tj. volbou v jednom grafu se ostatní příslušné grafy v pohledu na data upraví dle požadované volby automaticky.
17	Systém umožňuje 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 prohledávat okamžitě bez časových prodlev opětovného importu nebo dekomprimace starších dat, prohledávání dat nesmí vyžadovat manuální konfiguraci a zásahy uživatele.	Ano, Logmanager umožňuje 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 prohledávat okamžitě bez časových prodlev opětovného importu nebo dekomprimace starších dat, prohledávání dat nevyžaduje manuální konfiguraci a zásahy uživatele. Všechny operace uživatelů včetně prohledávání dashboardů jsou logované a lze je auditovat přímo v systému.
18	Systém provádí 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, manuální aktualizace a umožňuje používat tuto funkci jen pro vybrané IP adresné prostory. Doložte odkazem na dokumentaci, jakým způsobem se požadované funkce v grafickém rozhraní systému nastavují.	Ano, Logmanager provádí 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, manuální aktualizace a umožňuje používat tuto funkci jen pro vybrané IP adresné prostory. Dokumentace zde: https://doc.logmanager.com/latest/cz/web-interface/network/dns/
19	Systém podporuje nativní získávání logů z Office365/Microsoft365 prostředí bez ohledu na použitou licenci 365 prostředí a bez nutnosti instalovat dodatečné externí komponenty. Požadujeme předložit link na dokumentaci popisující nastavení systému v jednotném grafickém rozhraní tak, aby získával logy z Office365/Microsoft365.	Ano, Logmanager podporuje nativní získávání logů z Office365/Microsoft365 prostředí bez ohledu na použitou licenci 365 prostředí a bez nutnosti instalovat dodatečné externí komponenty. Dokumentace zde: https://doc.logmanager.com/latest/cz/web-interface/sources/ (záložka Office 365)
20	V případě krátkodobého (do 10 minut) až dvounásobného přetížení systému proti jeho tabulkovým hodnotám nesmí dojít ke ztrátě logů nebo nesprávnému stanovení časového razítka. Všechny přijaté nezpracované logy/události musí být ukládány do vyrovnávací paměti.	Ano, Logmanager zajistí, v případě krátkodobého (do 10 minut) až dvounásobného přetížení systému proti jeho tabulkovým hodnotám, že nedojde ke ztrátě logů nebo nesprávnému stanovení časového razítka. Všechny přijaté nezpracované logy/události jsou ukládány do vyrovnávací paměti.
21	Systém musí umožňovat unifikované vyhledávání napříč všemi typy dat a zařízeními dle normalizovaných polí (uživatelské jméno, zdrojová IP, značka/tag apod.).	Ano, Logmanager umožňuje unifikované vyhledávání napříč všemi typy dat a zařízeními dle normalizovaných polí (uživatelské jméno, zdrojová IP, značka/tag apod.).
22	Systém musí mít možnost uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování. Továrně dodané pohledy na data nesmí jít administrátorem ani uživatelem systému nevratně modifikovat nebo smazat.	Ano, Logmanager umožňuje uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování. Továrně dodané pohledy na data nelze administrátorem ani uživatelem systému nevratně modifikovat nebo smazat.
23	Systém obsahuje 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, Logmanager obsahuje reportovací nástroj s přednastavenými nejběžnějšími reporty a možností vlastních úprav a vytvoření nových pohledů. Pro vytváření nových pohledů na data nelze používat SQL jazyk.
24	Systém obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění.	Ano, Logmanager obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění.
25	Na základě pohledu na uložená data lze provést export dat ve strukturovaném formátu tak, jak jsou v továrně nastaveném nebo uživatelsky nastaveném pohledu data skutečně zobrazena.	Ano, Logmanager zajišťuje, že na základě pohledu na uložená data lze provést export dat ve strukturovaném formátu tak, jak jsou v továrně nastaveném nebo uživatelsky nastaveném pohledu data skutečně zobrazena.
26	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. Požadujeme předložit link na online dokumentaci nebo připojit pdf aktuální kompletní dokumentace k ověření jednotlivých vlastností navrhovaného systému.	Ano, konfigurační a systémové rozhraní a dokumentace k těmto rozhraním je identické v anglickém i v českém jazyce. Není zahrnuta omezená dokumentace v českém jazyce nebo zjednodušená dokumentace odkazující na další dokumentaci v anglickém jazyce, případně na dokumentaci třetích stran. Dokumentace zde: https://doc.logmanager.com/latest/cz/
27	Systém umožňuje kapacitní i výkonovou škálovatelnost.	Ano, Logmanager nabízí kapacitní i výkonovou škálovatelnost.
28	Čistá kapacita úložného prostoru (kapacita diskového pole) dostupná pro uložená data nabízeného systému musí být minimálně 40TB dat.	ANO, čistá kapacita úložného prostoru (kapacita diskového pole) dostupná pro uložená data nabízeného systému je 109TB dat.
29	Požadujeme, aby ze systému bylo možné za běhu vytáhnout libovolné dva disky, bez ztráty dat a vlivu na funkčnost řešení. Redundance disků nesmí ovlivňovat požadovanou kapacitu úložiště.	ANO, díky konfiguraci RAID je možné za běhu vytáhnout libovolné dva disky, bez ztráty dat a vlivu na funkčnost řešení. Redundance disků neovlivňuje požadovanou kapacitu úložiště.
30	Pokročilá telemetrie a monitoring stavu systému. Systém musí umět zobrazovat kromě běžných telemetrických dat o svojí činnosti i data ohledně rychlosti indexování, délce fronty dat čekající na zpracování a rychlosti odezvy DNS serverů vyřizujících DNS PTR odpovědi. Dále musí umožňovat alertování při překročení prahových hodnot nebo chybě systému, s odesláním upozornění pomocí SMTP nebo Syslogu.	ANO, Logmanager obsahuje pokročilou telemetrii a monitoring stavu systému. Systém umí zobrazovat kromě běžných telemetrických dat o svojí činnosti i data ohledně rychlosti indexování, délce fronty dat čekající na zpracování a rychlosti odezvy DNS serverů vyřizujících DNS PTR odpovědi. Dále umožňuje alertování při překročení prahových hodnot nebo chybě systému, s odesláním upozornění pomocí SMTP nebo Syslogu.

31	Jednotná centrální webová konzole 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 nebo aby se konfigurace musela provádět mimo jednotné webové rozhraní. Požadujeme předložit dokumentaci, ze které je zřejmé, jakým způsobem je realizována konfigurace v rámci jednotné konzole.	Ano, Logmanager obsahuje 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. Logmanager nemá více rozdílných konzolí od různých výrobců s rozdílným ovládáním. Konfigurace se neprovádí mimo jednotné webové rozhraní. Dokumentace zde: https://doc.logmanager.com/latest/cz/ A webové rozhraní konzole: https://doc.logmanager.com/latest/cz/web-interface
32	Požadujeme, aby systém umožňoval jednotné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem na základě typu zdrojů a značek a k jednotlivým ovládacím komponentům systému. Připojte odkaz na dokumentaci popisující vytváření uživatelských rolí v grafickém rozhraní systému.	Ano, Logmanager umožňuje jednotné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem na základě typu zdrojů a značek a k jednotlivým ovládacím komponentům systému. Systémové skupiny: https://doc.logmanager.com/latest/web-interface/users/system-groups/ Databázové skupiny: https://doc.logmanager.com/latest/web-interface/users/database-groups
33	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, Logmanager obsahuje ucelené all-in-one řešení pro parsování a normalizaci přijatých událostí bez nutnosti dodatečné instalace externích aplikací nebo systémů. Monitorování systémů Windows probíhá pomocí agentů.
34	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, Logmanager podporuje ověřování uživatele systému na externím LDAP serveru. V případě výpadku externího LDAP systému podporuje ověření lokálního účtu. Systém automaticky zaznamenává uživatelská jména u akcí provedených konkrétním uživatelem.
Minimální HW parametry požadovaného systému		
35	Jedna hardwarová appliance o velikosti max. 2U, včetně lyžin umožňujících vysunutí zapnutého systému z racku pro servisní účely.	Ano, Logmanager je jedna hardwarová appliance o velikosti max. 2U, včetně ramena pro kabelový management umožňujícího vysunutí zapnutého systému z racku pro servisní účely.
36	HW appliance obsahuje veškeré potřebné komponenty (CPU, RAM, diskový prostor) pro svoji činnost a je nezávislá na dalších systémech.	Ano, HW appliance obsahuje veškeré potřebné komponenty (CPU, RAM, diskový prostor) pro svoji činnost a je nezávislá na dalších systémech
37	2 procesory, min. 16 jader každý, s podporou HyperThreadingu nebo Multi-Threadingu.	Ano, Logmanager obsahuje 2 procesory, 16 jader každý, s podporou HyperThreadingu
38	Min. 128GB DDR-4 a možnost rozšíření o NVMe paměťové pole pro zpracování dat v čase blízkém reálnému (Near Real-Time).	Ano, Logmanager obsahuje 128 GB DDR-4 a možnost rozšíření o NVMe paměťové pole pro zpracování dat v čase blízkém reálnému (Near Real-Time).
39	Minimálně 40TB pro integrovanou databázi podporovanou HW akcelerovaným SAS RAID řadičem s read-write cache min. 8GB. Řadič diskového pole musí obsahovat zálohovací baterii nebo být vybaven flash pamětí.	Ano, Logmanager obsahuje 109 TB pro integrovanou databázi podporovanou HW akcelerovaným SAS RAID řadičem s read-write cache 8 GB. Řadič diskového pole obsahuje zálohování.
40	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, Logmanager obsahuje 12 ks stejných RAID edition disků určených pro použití v datacentrech, o rychlosti minimálně 7200 otáček/m.
41	Minimálně 4x 1Gbit LAN porty + 1x dedikovaný 1Gbit port pro management HW. Konfigurace všech parametrů síťového rozhraní včetně link agregace dle LACP (802.3ad), VLAN a IP adresace v jednotném webovém rozhraní systému.	Ano, Logmanager obsahuje 4x 1Gbit LAN porty + 1x dedikovaný 1Gbit port pro management HW. Konfigurace všech parametrů síťového rozhraní včetně link agregace dle LACP (802.3ad), VLAN a IP adresace v jednotném webovém rozhraní systému
42	Ventilátory redundantní a vyměnitelné za provozu.	Ano, větráky v systému jsou vyměnitelné za provozu a redundantní.
43	Napájecí zdroje redundantní a vyměnitelné za chodu (hotplug).	Ano, Logmanager obsahuje 2x napájecí zdroje s redundancí napájení 1+1. Zdroje jsou vyměnitelné za provozu.
44	Virtuální KVM (tj. převzetí textové i grafické konzole serveru a zajištění přenosu povelů z klávesnice a myši vzdáleného počítače.	Ano, virtuální KVM v Logmanageru umožňuje převzetí textové i grafické konzole serveru a zajištění přenosu povelů z klávesnice a myši vzdáleného počítače.
45	Systém pro vzdálenou správu serveru včetně potřebné licence, pokud je třeba (obdobá HP iLO, Dell iDRAC apod).	Ano, Logmanager obsahuje Dell iDRAC.
Výkonnostní a SW parametry systému		
46	Systém funguje formou HW appliance (všechny části systémů je možné nastavit v centrální webové konzoli a není nutné editovat žádné konfigurační soubory, scripty nebo makra v příkazové řádce).	Ano, Logmanager funguje formou HW appliance (všechny části systémů je možné nastavit v centrální webové konzoli a není nutné editovat žádné konfigurační soubory, scripty nebo makra v příkazové řádce).
47	Aktualizace systému jsou distribuovány v jednotném balíku a jejich instalace je prováděna uživatelsky přes centrální webovou správcovskou 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, aktualizace systému jsou distribuovány v jednotném balíku a jejich instalace je prováděna uživatelsky přes centrální webovou správcovskou konzoli. Všechny aktualizace jsou prováděny z webového prostředí bez potřeby asistence dodavatele/výrobce dodávaného systému. Odkaz na poznámky zde: https://doc.logmanager.com/latest/cz/introduction/release-notes/

48	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, nebo přiložte odkaz na dokumentaci s detailním popisem.	Ano, Logmanager podporuje downgrade v jednom kroku, pro případ problémů s novou verzí systému po upgrade. Downgrade je možný bez součinnosti výrobce. Dokumentace zde: https://doc.logmanager.com/latest/cz/additional-informations/logmanager-software-downgrade
49	Průměrný trvalý příjem min. 5000 událostí/s. Výkon musí být dosažen na požadované množství událostí s průměrnou délkou zpráv minimálně 700Byte trvale. Systém musí prokazatelně kompletně zpracovat přijaté události včetně vytváření očekávaných metadat (DNS-PTR, čísla a jména ASN, geolokace), zajišťovat normalizaci, zamezovat ztrátě přijatých událostí nebo posunutí důvěryhodného časového razítka oproti času skutečného příjmu každé události.	Ano, Logmanager zajišťuje průměrný trvalý příjem min. 10000 událostí/s. Výkon je dosažen na požadované množství událostí s průměrnou délkou zpráv minimálně 700Byte trvale. Systém kompletně zpracuje přijaté události včetně vytváření očekávaných metadat (DNS-PTR, čísla a jména ASN, geolokace), zajišťuje normalizaci, zamezuje ztrátě přijatých událostí nebo posunutí důvěryhodného časového razítka oproti času skutečného příjmu každé události.
50	Špičkový příjem minimálně 10000 událostí/s po dobu nejméně 10 minut a průměrnou délkou minimálně 700byte. Systém musí prokazatelně kompletně zpracovat přijaté události, zamezovat ztrátě ukládaných dat nebo posunutí důvěryhodného časového razítka oproti času skutečného příjmu zpráv. Při zpracování dat během špičkového příjmu akceptujeme zpoždění zobrazení zpracovávaných dat. Systém ani ve špičkovém výkonu nesmí dovolit ztrátu dat, skluz důvěryhodného časového razítka nebo jiné prokazatelné vady na zpracovávaných datech oproti zpracování při průměrném trvalém příjmu událostí.	Ano, Logmanager zajišťuje příjem 20000 událostí/s po dobu nejméně 10 minut a průměrnou délkou minimálně 700byte. Systém zpracuje přijaté události, zamezuje ztrátě ukládaných dat nebo posunutí důvěryhodného časového razítka oproti času skutečného příjmu zpráv. Při zpracování dat během špičkového příjmu je možné zpoždění zobrazení zpracovávaných dat. Systém ani ve špičkovém výkonu nedovolí ztrátu dat, skluz důvěryhodného časového razítka nebo jiné prokazatelné vady na zpracovávaných datech oproti zpracování při průměrném trvalém příjmu událostí.
51	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, Logmanager má neomezený počet zařízení pro příjem zasílaných událostí včetně neomezeného množství událostí v GB. Integrovaná databáze má čistou velikost 109 TB a podporuje kompresi ukládaných dat.
52	Uživatelská konfigurace klasifikace dat, parserů, filtrů a alertů se provádí pomocí vizuálního programovacího jazyka v centrální správcovské webové konzoli. Vizuální programovací jazyk musí uživateli umožnit psát konfigurace bez nutnosti znalosti programování (např. Node-RED, Microsoft VPL, Blockly apod). Vizuální programovací jazyk není prezentován textově, ale graficky formou schémat-symbolů, které reprezentují aplikační logiku a kontrolují syntaxi. Doložte odkazem na dokumentaci systém vizuálního programování a popisu jednotlivých použitých komponent vizuálního programování nástroje.	Ano, uživatelská konfigurace klasifikace dat, parserů, filtrů a alertů se provádí pomocí vizuálního programovacího jazyka v centrální správcovské webové konzoli. Vizuální programovací jazyk umožňuje uživateli psát konfigurace bez nutnosti znalosti programování (např. Node-RED, Microsoft VPL, Blockly apod). Vizuální programovací jazyk není prezentován textově, ale graficky formou schémat-symbolů, které reprezentují aplikační logiku a kontrolují syntaxi. Dokumentace zde: https://doc.logmanager.com/latest/cz/web-interface/parser/parsing-rules/
53	Konfigurace uživatelských parserů musí umožňovat automatické doplňování DNS reverzních záznamů, GeoIP informace a identifikace výrobce zařízení podle MAC adresy.	Ano, konfigurace uživatelských parserů musí umožňovat automatické doplňování DNS reverzních záznamů, GeoIP informace a identifikace výrobce zařízení podle MAC adresy.
54	Možnost on-line ladění uživatelsky definovaných parserů - při jejich vytváření je možné vložit skupinu testovacích zpráv, při změně je okamžitě zobrazena výsledná podoba rozparsovaných 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. Doložte 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, Logmanager umožňuje on-line ladění uživatelsky definovaných parserů - při jejich vytváření je možné vložit skupinu testovacích zpráv, při změně je okamžitě zobrazena výsledná podoba rozparsovaných dat a případná chybová hlášení s upozorněním na chybná místa vytvářeného parseru. Pro snadnější vytváření parserů je zde možnost vložit minimálně 20 testovacích zpráv současně. Dokumentace zde: https://doc.logmanager.com/latest/cz/web-interface/parser/parsing-rules/
55	V centrální správcovské konzoli je možné 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, v centrální správcovské konzoli Logmanageru je možné 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.
56	Všechny přidávané značky jsou ukládány s každou přijatou událostí, na základě značky je možné filtrovat data nebo omezovat oprávnění uživatelů systému k jednotlivým událostem.	Ano, všechny přidávané značky jsou ukládány s každou přijatou událostí, na základě značky je možné filtrovat data nebo omezovat oprávnění uživatelů systému k jednotlivým událostem.

57	Pro budoucí nasazení ve vysoké dostupnosti a výkonnosti rozšíření je vyžadována podpora sestavení ve vysoké dostupnosti – požadujeme podporu minimálně 4 nodů v clusteru. 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. Doložte odkazem na dokumentaci, jakým způsobem se cluster vytváří a jakým způsobem se provádí obnovení po možném výpadku jednotlivých zúčastněných komponent.	Ano, v rámci budoucího nasazení ve vysoké dostupnosti a výkonnosti rozšíření je podpora sestavení ve vysoké dostupnosti – Logmanager zajišťuje podporu minimálně 4 nodů v clusteru. Nastavení clusteru se kompletně realizuje v grafickém rozhraní správcovské konzole v jednom kroku, nelze konfigurovat sestavení scripty, makry nebo úpravou textové konfigurace systému a pomocí ručních restartů služeb. Systém ve vysoké dostupnosti přehledně informuje o stavu clusteru a procesu synchronizace databází. Dokumentace k realizaci vysoké dostupnosti je kompletní a popisovat všechny kroky sestavování a obnovení v případě výpadku komponenty clusteru. Odkaz na dokumentaci zde: https://doc.logmanager.com/latest/cz/web-interface/system/cluster
58	Vícenodový cluster se chová i ovládá jako jednotný systém, nutnost nezávislé konfigurace na každé jednotce v clusteru je vyloučena. Vícenodový cluster umožňuje geolokační oddělení a pro komunikaci v rámci clusteru musí využívat definovaný TCP/UDP port pro snadné nastavení prostupu firewallu. Veškerá komunikace v rámci clusteru musí být šifrovaná s vysokým kryptografickým standardem pro bezpečné vytvoření privátní virtuální sítě na síťové vrstvě. Popište použitou technologii zabezpečení komunikace v rámci clusteru.	Ano, Logmanager využívá pro bezpečné sestavení clusteru i komunikaci s Logmanager Forwardery pevně dané kryptografické algoritmy: pro dohodu na klíči používá Diffieho–Hellmanův protokol s využitím eliptických křivek s křivkou Curve25519, samotné šifrování má podobu autentizovaného šifrování šifrou ChaCha20 a autentizační funkcí Poly1305 s hašovací funkcí BLAKE2. Pro klíče hašovacích tabulek používá SipHash. Použitý je UDP port 51820 pro Cluster a UDP port 51821 pro komunikaci Logmanager <-> Logmanager Forwarder.
59	V případě rozšíření systému na cluster musí navrhovaný systém zajistit bezvýpadkovost sběru logů.	Ano, v případě rozšíření systému na cluster Logmanager zajistí bezvýpadkovost sběru logů.
60	Řešení musí umožňovat rozšíření mezipaměti diskového subsystému o SSD nebo NVRAM typu o kapacitě minimálně 6TB.	Ano, Logmanager umožňuje rozšíření mezipaměti diskového subsystému o SSD nebo NVRAM typu o kapacitě minimálně 6 TB.
61	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, Logmanager umožňuje 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.
62	Podpora zálohování nebo obnovení konfigurace v jednom kroku a jednom souboru pro celý systém. Doložte odkazem na dokumentaci, jakým způsobem se provádí zálohování a obnova konfigurace systému.	Ano, Logmanager podporuje zálohování nebo obnovení konfigurace v jednom kroku a jednom souboru pro celý systém. Odkaz na dokumentaci zde: https://doc.logmanager.com/latest/cz/web-interface/system/backup-restore/
63	Podpora důvěryhodného zálohování dat na externí systém. Požadováno plánované i ad-hoc zálohování. Zálohy dat musejí být vhodně kompresovány a umožnit v budoucnosti obnovení bez ohledu na verzi systému, ve které byla záloha pořízena. Doložte odkazem na dokumentaci, jakým způsobem se realizuje zálohování a obnova záloh.	Ano, Logmanager podporuje důvěryhodného zálohování dat na externí systém. Zajišťuje plánované i ad-hoc zálohování. Zálohy dat jsou vhodně kompresovány a umožňují v budoucnosti obnovení bez ohledu na verzi systému, ve které byla záloha pořízena. Odkaz na dokumentaci zde: https://doc.logmanager.com/latest/cz/web-interface/system/backup-restore/
Alerty		
64	Systém je schopen na základě uživatelsky zadaných podmínek splněných v přijatých datech vygenerovat alert.	Ano, Logmanager je schopen na základě uživatelsky zadaných podmínek splněných v přijatých datech vygenerovat alert.
65	Text emailu vygenerovaného alertem musí být uživatelsky definovatelný s proměnnými, které jsou vyplněny z přijaté rozparsované události.	Ano, text e-mailu vygenerovaného alertem je uživatelsky definovatelný s proměnnými, které jsou vyplněny z přijaté rozparsované události. Logmanager umí zobrazovat počet odesílaných e-mailů ve frontě.
66	Systém musí obsahovat výrobcem předpřipravené sety/vzory alertů a korelací.	Ano, Logmanager obsahuje výrobcem předpřipravené sety/vzory alertů a korelací.
67	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. Doložte odkazem na dokumentaci, jakým způsobem realizujete konfiguraci a testování alertů a korelací.	Ano, Logmanager provádí 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 umožňuje okamžitou kontrolu funkčnosti výstupu alertu nebo korelace vložení příslušné testovací zprávy, včetně zobrazení upozornění na případné uživatelské chyby. Odkaz na dokumentaci zde: https://doc.logmanager.com/latest/cz/additional-informations/events-processing-in-blockly/defined-xml-blocks/special-blocks/special-elements/send-alert/

68	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. Doložte odkazem na dokumentaci, jakým způsobem se zpráva, která vyvolala spuštění alertu, odesílá na externí systém a jak se definuje formát odesílání dat.	Ano, jako výstupní pravidlo alertu Logmanager umí odeslat událost, která alert vyvolala, na externí systém minimálně prostřednictvím SMTP nebo Syslogu přes TCP protokol. U Syslog protokolu je možnost definice formátu odesílaných dat pro snazší integraci se systémy třetích stran. Odkaz na dokumentaci zde: https://doc.logmanager.com/latest/web-interface/logs/syslog-output/
69	V alertech je možné nejen využívat, ale i přiřazovat značky (příklad: pošli alert jen v případě, že se událost stala na kritickém serveru a je označen názvem lokality, nebo pokud událost obsahuje podmínku, přiřaď novou značku). Doložte odkazem na dokumentaci, jakým způsobem lze v jednotném grafickém rozhraní systému definovat a přiřazovat značky.	Ano, v alertech je možné nejen využívat, ale i přiřazovat značky (příklad: pošli alert jen v případě, že se událost stala na kritickém serveru a je označen názvem lokality, nebo pokud událost obsahuje podmínku, přiřaď novou značku). Odkaz na dokumentaci zde: https://doc.logmanager.com/latest/cz/additional-informations/events-processing-in-blockly/defined-xml-blocks/data-structures-blocks/message-add-tag/
70	Systém podporuje 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 zobrazení výsledku testu o provedené akci.	Ano, systém podporuje základní funkce SIEM - funkce pro korelace událostí a upozornění s hraničními limity. Definice korelačních pravidel je prováděna pomocí vizuálního programovacího jazyka a obsahuje možnost vložení testovací zprávy a zobrazení výsledku testu o provedené akci
Sběr událostí z Microsoft prostředí		
71	Události z Microsoft prostředí jsou vyčítány pomocí agenta instalovaného přímo v koncových systémech. Windows agent musí současně podporovat jak monitoring interních windows logů, tak monitoring textových souborových logů. Agent se nesmí instalovat individuálně, ale prostřednictvím MS AD Group Policy a nesmí vyžadovat žádnou konfiguraci na cílovém systému. Doložte odkaz na dokumentaci popisující požadované vlastnosti integrovaného Windows agenta.	Ano, události z Microsoft prostředí jsou vyčítány pomocí agenta instalovaného přímo v koncových systémech. Windows agent současně podporuje jak monitoring interních Windows logů, tak monitoring textových souborových logů. Agent se neinstaluje individuálně, ale prostřednictvím MS AD Group Policy a nevyžaduje žádnou konfiguraci na cílovém systému. Odkaz na dokumentaci zde: https://doc.logmanager.com/latest/cz/logmanager-beats-agent/logmanager-orchestrator/
72	Agent sběru z Microsoft podporuje globální i lokální nastavení filtrace odesílaných událostí pomocí centrální správcovské konzole. Například, zašli pouze logy z adresářů eventview Systém, Security, Sysmon a Terminal Services a zahod' logy s EventId 7036.	Ano, agent sběru z Microsoft podporuje globální i lokální nastavení filtrace odesílaných událostí pomocí centrální správcovské konzole. Například, zašli pouze logy z adresářů eventview Systém, Security a Terminal Services a zahod' logy s EventId 7036.
73	Filtrace odesílaných událostí agenty se konfiguruje pomocí vizuálního programovacího jazyka z centrální správcovské 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. Doložte odkazem na dokumentaci, jakým způsobem se vytváří a přiřazují filtry pro Windows agenty pro sběr logů a jakým způsobem se testuje účinnost filtru.	Ano, filtrace odesílaných událostí agenty se konfiguruje pomocí vizuálního programovacího jazyka z centrální správcovské 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. Odkaz na dokumentaci zde: https://doc.logmanager.com/latest/cz/logmanager-beats-agent/beats-agents
74	Windows agent nevyžaduje 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. Tj. vlastní správa a aktualizace Windows agenta se neprovádí z Group Policy.	Ano, Windows agent nevyžaduje administrátorské zásahy na koncovém systému – je centrálně spravovaný a jeho konfigurace je kompletně realizována v grafickém rozhraní systému bez využití skriptů nebo maker. Konfigurace je automaticky distribuována přímo z centrální konzole systému., tj. vlastní správa a aktualizace Windows agenta se neprovádí z Group Policy.
75	Komunikace Windows agenta a centrálního systému musí být zabezpečena TLS 1.2 a výše a musí podporovat ověřování certifikátem.	Ano, komunikace Windows agenta a centrálního systému je zabezpečena TLS 1.2 a podporuje ověřování certifikátem.
76	Windows agent podporuje 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 a logy rozšířit Sysmonem. Dále musí Windows agent podporovat centralizované nastavení z administrátorské konzole systému pro sběr textových logů včetně možnosti výběru jejich formátu. Doložte odkazem na dokumentaci, jakým způsobem se nastavují parametry sběru logů globálně a jakým způsobem u konkrétního agenta.	Ano, Windows agent podporuje 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 a logy rozšířit Sysmonem. Dále Windows agent podporuje nastavení z administrátorské konzole systému pro sběr textových logů včetně možnosti výběru jejich formátu. Odkaz na dokumentaci: https://doc.logmanager.com/latest/cz/logmanager-beats-agent/beats-agents/
77	Počet instalací Windows agenta nesmí být licenčně a časově omezen. Předpokládáme instalaci agentů na všechny systémy současně, proto je nutné potvrdit, zda systém výkonnostně splňuje tento požadavek. Jedná se o klíčovou funkci, proto budeme před uzavřením smlouvy požadovat předvedení požadovaných funkcí, stability i výkonnostní kapacity nabízeného systému pro sběr logů z prostředí Microsoft.	Ano, počet instalací Windows agenta není licenčně a časově omezen a výkonnostně (tj. instalací na všechny systémy) splňuje předpokládaný rozsah nasazení.
Podpora pro sběr událostí z poboček		

78	Systém musí obsahovat centrálně spravované řešení, které sbírá události na pobočkách a umožní jejich odeslání po saturované lince bez ztráty dat. Doložte odkazem na dokumentaci, jakým způsobem realizujete sběr událostí z poboček.	Ano, Logmanager obsahuje centrálně spravované řešení, tzv. Logmanager Forwarder, které sbírá události na pobočkách a umožní jejich odeslání po saturované lince bez ztráty dat. Odkaz na dokumentaci: https://doc.logmanager.com/latest/cz/web-interface/sources/forwarder/
79	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, Logmanager podporuje centralizovanou správu pro sběr událostí přímo z centrálního úložiště dat včetně dokumentace požadavků na virtualizaci a komunikační matici pro šifrovaný přenos dat. Odkaz pro další dokumentaci je: https://doc.logmanager.com/latest/cz/web-interface/sources/forwarder/
80	Řešení musí být schopno automaticky navázat spojení s centrálním úložištěm dat a přenášena data šifrovat. V případě výpadku spojení mezi pobočkou a centrálou musí spojení automaticky obnovit.	Ano, Logmanager Forwarder umí automaticky navázat spojení s centrálním úložištěm dat a přenášena data šifrovat. V případě výpadku spojení mezi pobočkou a centrálou umí spojení automaticky obnovit.
81	Řešení musí komunikovat po definovaném TCP/UDP portu, aby mohl být snadno nastaven přístup přes firewall a řešena kvalita služby (QoS) pro přenos událostí. Doložte odkazem na dokumentaci, jak vypadá komunikační matice pro připojení řešení pro sběr událostí na pobočkách.	Ano, Logmanager Forwarder komunikuje po definovaném TCP/UDP portu, aby mohl být snadno nastaven přístup přes firewall a řešena kvalita služby (QoS) pro přenos událostí. Odkaz na dokumentaci: https://doc.logmanager.com/latest/cz/additional-informations/communication-of-logmanager/
82	Řešení musí poskytovat kapacitu vyrovnávací paměti pro minimálně 100GB událostí, které na pobočce mohou vzniknout během výpadku spojení mezi pobočkou a datovým centrem.	Ano, Logmanager Forwarder disponuje kapacitou vyrovnávací paměti pro minimálně 100 GB událostí, které na pobočce mohou vzniknout během výpadku spojení mezi pobočkou a datovým centrem.
83	Řešení pro sběr dat z poboček musí mít výkon minimálně 5 tisíc událostí/s, a to i v trvalé zátěži.	Ano, Logmanager Forwarder má výkon minimálně 5 tisíc událostí/s, a to i v trvalé zátěži.
84	Řešení musí poskytnout podporu pro sběr událostí na identických UDP i TCP portech jako hlavní dodaný systém.	Ano, Logmanager Forwarder poskytuje podporu pro sběr událostí na identických UDP i TCP portech jako hlavní dodaný systém.
85	Řešení musí být k dispozici jako fyzický systém nebo jako virtuální systém pro VMware ESXi a Hyper-V.	Ano, Logmanager Forwarder je k dispozici jako fyzický systém nebo jako virtuální systém pro VMware ESXi a Hyper-V.
86	Řešení musí být schopno komunikovat z pobočky na centrálu i přes vícenásobný překlad adres (NAT).	Ano, Logmanager Forwarder komunikuje z pobočky na centrálu i přes vícenásobný překlad adres (NAT).
Vysoká dostupnost, SW Podpora a záruka na hardware		
87	Požadujeme volitelnou podporu pro nasazení ve vysoké dostupnosti.	Ano, je nabídnutá podpora pro nasazení ve vysoké dostupnosti.
88	HW - Požadovaná minimálně 5letá servisní podpora na hardware appliance s opravou v místě instalace serveru a s garantovanou odezvou následující pracovní den od nahlášení případné závady.	Ano, součástí nabídky je 5letá servisní podpora na hardware appliance s opravou v místě instalace serveru a s garantovanou odezvou následující pracovní den od nahlášení případné závady.
89	Systém musí podporovat vygenerování TSR (technického support reportu) pro možnost diagnostiky bez vzdáleného přístupu.	Ano, Logmanager podporuje vygenerování TSR (technického support reportu) pro možnost diagnostiky bez vzdáleného přístupu.
90	SW - Podpora výrobce na aktualizaci systému a parserů na 5 let. Podpora musí obsahovat aktualizaci SW minimálně 4x ročně, opravy chyb a telefonickou a emailovou podporu s diagnostikou vzdáleným přístupem.	Ano, součástí nabídky je podpora výrobce na aktualizaci systému a parserů na 5 let. Podpora obsahuje aktualizaci SW minimálně 4x ročně, opravy chyb a telefonickou a e-mailovou podporu s diagnostikou vzdáleným přístupem.
Technická kvalifikace dle § 79 odst. 2 písm. b) a k) zákona a způsob jejího prokázání		

91	Účastník zadávacího řízení předloží dle § 79 odst. 2 písm. b) zákona seznam významných dodávek obsahující minimálně 2 významné obdobné dodávky poskytnuté za poslední 3 roky před zahájením zadávacího řízení včetně uvedení ceny bez DPH, doby jejího poskytnutí a identifikace objednatele. Za významnou obdobnou dodávku se v tomto případě považuje jednorázová dodávka zahrnující instalaci a konfiguraci jádra systému Log Managementu, kterým se rozumí kombinace hardware a software společně tvořících samostatný funkční celek, pro objednatele s minimálním počtem zdrojů logů 2000, přičemž minimální finanční objem bez DPH této dodávky musí činit alespoň 1 000 000,- Kč.	Název zakázky č. 1: Pořízení a implementace nástroje pro LogManagement Předmět zakázky: Dodávka, instalace a zprovoznění Logmanageru Finanční objem: 3 859 900 Kč bez DPH Doba realizace: 09/2024 – 10/2024 Objednatel: Fakultní Thomayerova nemocnice Vítěnská 800, 140 00 Praha 4 IČ: 00064190 Ing. Martin Gonda, vedoucí odboru telematiky, 733 164 332, martin.gonda@ftn.cz Název zakázky č. 2: Kontrolní správa provozních logů 2025+ Předmět zakázky: Dodávka, instalace a zprovoznění Logmanageru Finanční objem: 2 890 400 Kč bez DPH Doba realizace: 12/2024 – 01/2025 Objednatel: Ministerstvo zemědělství České republiky Těšnov 65/17, 110 00 Praha 1 IČ: 00020478 Ing. Aleš Prokeš, vedoucí oddělení provozu, 602 227 991, Ales.Prosek@mze.gov.cz
93	Účastník zadávacího řízení předloží dle § 79 odst. 2 písmene c) zákona seznam techniků nebo technických útvarů, které se budou podílet na plnění veřejné zakázky.	Jan Frank Matěj Šimáček
94	Technický specialista produktů log managementu – nejméně 2 osoby splňující následující požadavky: praxe v oblasti implementace logmanagementu minimálně 3 roky před zahájením zadávacího řízení, každá z osob je držitelem platného certifikátu.	Obě výše uvedené osoby splňující následující požadavky: praxe v oblasti implementace logmanagementu minimálně 3 roky před zahájením zadávacího řízení, každá z osob je držitelem platného certifikátu (certifikáty jsou přiloženy k nabídce)
Další požadavky zadavatele		
95	• vyzvat uchazeče k poskytnutí funkčních vzorků pro účely testování a ověření požadovaných funkčních vlastností. Uchazeč je povinen doručit testovací vzorky zadavateli do deseti (10) pracovních dnů od doručení výzvy k jejich poskytnutí, na adresu uvedenou v této výzvě. Vybraný uchazeč poskytne testovací vzorky bezplatně a na dobu minimálně následujících patnácti (15) pracovních dnů, rovněž po tuto dobu poskytne součinnost s testováním. Testovací vzorky budou dodány v identické konfiguraci s nabízeným systémem a zadavatel ve výzvě jasně stanoví, jaké vzorky za účelem hodnocení nabídek požaduje. Ověření funkčních vlastností nabízeného systému bude provádět zadavatel, vycházející z dokumentace k nabízenému systému. V případě nejasností zadavatel vyzve k účasti zástupce dodavatele/uchazeče, který mu poskytne potřebnou součinnost, a to maximálně do pěti (5) pracovních dnů po doručení výzvy uchazeči. Testy budou provedeny v prostředí zadavatele. Po ukončení testování budou funkční vzorky uchazeči vráceny (uchazeč si vyzvedne vzorky na vlastní náklady v místě plnění). Ověřování bude zakončeno vyhotovením zázpisu. V případě, že testovaný systém neprojde úspěšným	Uchazeč Compunet s.r.o s podmínkami Zadavatele souhlasí