**Název zakázky:** Systém log managementu pro sběr, ukládání a vyhodnocování událostí

**Číslo zakázky:** P21V00000039

**Zadavatel:** Statutární město Frýdek-Místek, se sídlem Frýdek-Místek, Radniční 1148, PSČ 738 01

1. **Cena dodávky**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Cena celkem bez DPH** | **DPH** | **Cena celkem včetně DPH** |
| Systém log managementu |  |  |  |
| Odborná podpora na 60 měsíců |  |  |  |
| **CELKEM** |  |  |  |

1. **Technická specifikace předmětu plnění veřejné zakázky**

Předmětem plnění veřejné zakázky je:

Dodávka, instalace a konfigurace nového (nepoužitého, nerepasovaného) systému log managementu pro sběr, ukládání a vyhodnocování událostí z kritických systémů a aplikací zadavatele. Zařízení a software musí být určeny pro český trh a musí splňovat minimálně níže uvedené technické a funkční parametry. Nabízené řešení musí obsahovat veškeré potřebné komponenty a licence pro funkčnost řešení jako celku. Veřejná zakázka zahrnuje dodávku (hardware, software včetně licencí a podpory), předprojektovou analýzu v místě plnění, kompletní implementaci, dodání technické a administrátorské dokumentace, otestování správné funkčnosti.

Další požadavky zadavatele:

* Zadavatel požaduje dodání originálních a nových zařízení, licencovaných ve jménu zadavatele a podle pravidel výrobce tak, aby bylo možné eskalovat případné závady přímo na lokální technickou podporu výrobce v českém nebo slovenském jazyce.
* Zboží musí být podporováno servisním střediskem výrobce na území České republiky.

Záruka a konzultace:

* Na nabízený systém je požadována záruka výrobce min. 60 měsíců bez dalších poplatků se zahájením opravy nejpozději následující pracovní den po nahlášení závady v místě instalace (NBD).
* Záruka na server musí být poskytnuta přímo výrobcem zařízení a musí být ověřitelná na veřejně přístupném webu výrobce.
* Při výměně vadného disku servis ani dodavatel nesmí vyžadovat vrácení pevného disku ani žádnou kompenzaci. Likvidace disku proběhne dle interních norem zadavatele.
* Garance aktualizací systému a parserů výrobcem min. 60 měsíců
* Poskytnutá záruka uvedená výše začíná platit od předání kompletního díla a podpisu akceptačních protokolů.
* Odborná podpora po dobu 60 měsíců v rozsahu 2 člověkohodin měsíčně, nevyčerpané hodiny se převádějí do dalšího období. Součástí je profylaxe systému, aktualizace, změny v nastavení pravidel, změny v nastavení konfigurací. Odborná podpora může mít formu telefonickou, písemnou, vzdálenou nebo v místě plnění.

1. **Systém log managementu pro sběr, ukládání a vyhodnocování událostí**

|  |  |  |
| --- | --- | --- |
| **Popis výrobku** | | |
| výrobce |  | |
| modelové označení |  | |
|  |  |  |
| **Požadované minimální parametry a vlastnosti** | | |
| Celistvý systém pro centralizovanou správu a analýzu událostí ze zdrojů organizace | | |
| Systém musí podporovat sběr událostí min. ve formátech Syslog (RFC5424), RAW, JSON (RFC7159), SNMP v3, Microsoft event log | | |
| Systém musí umožnit takové zabezpečení, aby nebylo možno mazat, měnit nebo editovat uložené logy | | |
| Systém musí konsolidovat logy na centrálním místě | | |
| Systém musí být kompletně obsluhován (konfigurace, administrace, přístup a práce s logy) pouze z jedné centrální konzole přístupné výhradně přes webové rozhraní s využitím HTTPS | | |
| Systém musí podporovat integraci s MS Active direktory pro ověřování uživatelů | | |
| Systém musí umožnit konfiguraci uživatelských rolí, na základě kterých je definovaná množina přístupových oprávnění jak k administraci systému, tak k přístupu a práci s logy | | |
| Systém musí obsahovat monitoring svého stavu s možností nastavení alertování pomocí SMTP při překročení mezních hodnot a chybách systému | | |
| Systém musí v centrální konzoli obsahovat nástroj pro reportování (musí být obsažena sada základních reportů a dále možnost úpravy a tvorby vlastních reportů) | | |
| Systém musí umožnit napojení na monitorovací systém PRTG pro další zpracování alertů a prahových hodnot | | |
| Systém musí umožnit generování alertů zasílaných pomocí SMTP na základě hodnot v přijatých datech jednotlivých logů, tyto aletry musí být uživatelsky definovatelné s proměnnými z přijaté rozparsované události | | |
| Součástí systému musí být vzory alertů nebo budou vytvořeny v rámci dodávky | | |
| Systém musí umožnit tvorbu alertů pomocí vizuálního programovacího jazyka grafickou formou obsahující aplikační logiku, programovací jazyk nesmí být prezentován textově | | |
| Systém musí umožnit v alertech využití filtrů a značek, filtry značky a podmínky musí být možno řetězit | | |
| Systém musí v centrální konzoli umožnit přidávání k jednotlivým zdrojům dat, aplikacím, zařízením, IP adresám, subnetům tzv. Značky, tyto Značky následně slouží pro snazší orientaci a práci se systémem, Značky mohou značit např. umístění, typ nebo důležitost zařízení | | |
| Systém musí umožnit na základě Značek filtrování dat nebo omezování přístupů uživatelům | | |
| Systém musí umožnit ukládání Značek s každou přijatou událostí | | |
| Systém musí umožnit v centrální konzoli při definování vlastního parseru možnost přidání Značky různé typy událostí (dostupný, nedostupný atd.) | | |
| Systém musí umožnit uživatelsky definované parsery dopsáním parseru pro zařízení uvedená v bodě 2.II bez nutnosti spolupráce s výrobcem nebo dodavatelem zařízení | | |
| Systém bude standardizovat přijaté logy do jednotného formátu a logy budou parsovány do příslušných políček podle jejich typu | | |
| Systém nad takto standardizovanými daty automaticky vytváří indexy pro rychlejší vyhledávání pro všechny políčka standardizovaného logu | | |
| Systém musí v centrální konzoli umožnit tvorbu vlastních parserů pomocí vizuálního programovacího jazyka, bez nutnosti znalosti programování a to grafickou formou obsahující aplikační logiku, programovací jazyk nesmí být prezentován textově | | |
| Systém musí umožnit on-line ladění uživatelsky definovaných parserů, kdy je při změně vidět okamžitě provedená změna rozparsovaných dat | | |
| Systém musí umožnit při konfiguraci uživatelských parserů automatické doplňování DNS reverzních záznamů a identifikace výrobce zařízení na základě MAC adresy | | |
| Systém musí umožnit snadné a rychle dostupné vyhledávání událostí | | |
| Systém musí umožnit unifikované vyhledávání skrze všechny typy dat a zařízení | | |
| Systém musí obsahovat předdefinované pohledy nad uloženými daty | | |
| Systém musí umožnit grafické znázornění událostí včetně zobrazení TOP událostí v definovaném časovém okně | | |
| Systém musí umožnit případné rozšíření do dalších poboček s tím, že na pobočce bude samostatné zařízení buďto jako HW box nebo virtuální systém v prostředí VMware vSphere 6.7 a vyšší | | |
| Komunikace mezi centrálním systémem a pobočkovým systémem musí probíhat šifrovaně, v případě výpadku spojení musí být obnoveno automaticky bez zásahu administrátora | | |
| Pobočkový systém musí poskytnou min. kapacitu 100 GB pro sběr událostí, které mohou vzniknout v době výpadku spojení mezi pobočkou a centrálním systémem | | |
| Pobočkový systém musí podporovat komunikaci přes UDP i TCP i přes NAT | | |
| Systém musí být ve shodě s požadavky normy ISO 27001:2013 pro pořizování auditních záznamů, potvrzení o shodě vystaveno autorizovanou osobou, nepostačuje čestné prohlášení | | |

|  |
| --- |
| **Sběr událostí z produktů Microsoft** |
| Systém musí umožnit vytěžování událostí z produktů Microsoft pomocí instalovaného agenta na koncovém systému. Agent musí podporovat monitoring interních logů z Windows, tak i monitoring souborových logů |
| Agent musí zajistit sběr nemodifikovaných událostí a detailní zpracování auditních informací |
| Agent musí umožnit nastavení filtrace odesílaných událostí pomocí centrální konzole |
| Filtrace odesílaných událostí se konfiguruje pomocí vizuálního programovacího jazyka z centrální konzole bez nutnosti znalosti programování a to grafickou formou obsahující aplikační logiku, programovací jazyk nesmí být prezentován textově |
| Agent v prostředí Windows nevyžaduje administrátorské zásahy na koncovém zařízení, agent musí být centrálně spravovaný a automaticky aktualizovatelný přímo z centrální konzole, agent se nespravuje a neaktualizuje pomocí GPO |
| Agent v prostředí Windows musí automaticky překládat zástupné kódy ve zprávách na text |
| Agent v prostředí Windows musí mít vyrovnávací paměť pro případ výpadku spojení mezi koncovým zařízením a centrálním systémem |
| Agent v prostředí Windows musí s centrálním systémem komunikovat šifrovaně |
| Agent v prostředí Windows musí automaticky doplňovat ke všem odesílaným událostem jejich textový popis, tak jak je originálně zobrazen v Event vieweru na koncových zařízeních |
| U agenta v prostředí Windows nesmí být licenčně omezen počet jejich instalací na koncové zařízení |

|  |
| --- |
| **HW a SW parametry systému** |
| Systém musí být dodán jako kompletní systém bez nutných dalších investic plně nezávislý na jiných systémech a to jako HW appliance, která bude umístěna v 19“ rackové skříni, součástí musí být cable management arm a ližiny pro možnost vytažení serveru z racku |
| HW appliance musí splňovat min. tyto parametry: 2 CPU s min. 10 fyzickými jádry; 64 GB RAM; 12 Gbps SAS RAID řadič s podporou RAID 0,1,5,6,10,50,60 s vyrovnávací pamětí min. 2GB zálohovaná baterií |
| Systém musí poskytnout min. 40 TB čisté kapacity pro ukládání dat, systém musí mít být odolný proti výpadku min. 2 disků tak, aby to nemělo dopad na funkčnost systému a celkovou kapacitu |
| Systém musí obsahovat redundantní napájecí zdroje a redundantní ventilátory – oba vyměnitelné za chodu systému |
| Server musí být spravovatelný přes vzdálenou správu serveru, licence (pokud je potřebná) musí být součástí dodávky |
| Systém musí obsahovat min. 2x SFP+ porty a 1x dedikovaný 1 Gbps port pro vzdálený management – součástí dodávky musí být i 2ks DAC kabelů v délce 1m kompatibilních pro připojení ke switchi HP 5900 PN: JC772A |
| Systém musí podporovat clustering a možnost rozšiřování kapacity přidáváním nodů do clusteru, kdy se systém musí neustále chovat jako jeden celek |
| Systém musí v případě rozšíření o další nody vystupovat pod jednou IP adresou |
| Systém musí zvládnout trvalý příjem min. 6.000 událostí za sekundu, ve špičce 10.000 událostí za sekundu, systém nesmí události zahazovat, musí umožnit uložení událostí do vyrovnávací paměti pro pozdější zpracování |
| Pobočkový systém musí zvládnout příjem min. 2.000 událostí za sekundu |
| Systém nesmí licenčně omezovat počet zařízení ani množství přijatých událostí v čase |

1. **Seznam min. podporovaných výrobců hardware, aplikací a operačních systémů**

|  |  |  |  |
| --- | --- | --- | --- |
| Apache httpd | HP | Microsoft Windows IIS | Ruckus |
| Apache Tomcat | HPE | Microsoft Windows Server | SAP |
| Aruba | Huawei | Microsoft Windows 10 | Sophos |
| Brocade FC switches | Juniper | Microsoft Sharepoint | Synology |
| Cisco | Linux | Microsoft-SQL | UBNT |
| Checkpoint | Microsoft Windows DHCP | MySQL | VMware |
| Dell | Microsoft Exchange | Oracle |  |
| Fortinet | Microsoft Windows Firewall | PostgreSQL |  |

1. **Implementace**

Uchazeč musí dodat plně funkční systém, kompletně zprovozněný, nainstalovaný, nakonfigurovaný a zapojený do infrastruktury zadavatele dle svých nejlepších znalostí a svědomí. Způsob implementace bude vycházet z předimplementační analýzy zpracované uchazečem před započetím instalace a konfigurace (náklady na provedení implementace musí být zahrnuty v nabídkové ceně).

- předimplementační analýza, která bude probíhat v místě plnění a u které budou přítomni zaměstnanci zadavatele z odboru IT

- předimplementační analýza bude mít jako výstup dokument ve formátu DOCX a mimo jiné musí obsahovat systémy, ze kterých bude sběr a ukládání logů probíhat, způsob napojení, nastavení atd.

- předimplementační analýza musí být zpracována před zahájením realizace instalace a konfigurace systému

- předimplementační analýza musí být předaná zadavateli a schválená zadavatelem, bez předané a odsouhlasené předimplementační analýzy nemůže započít instalace a konfigurace

- instalace a konfigurace musí probíhat prostřednictvím pracovníka uchazeče primárně přímo v místě plnění za přítomnosti zaměstnance zadavatele z odboru IT, a to v pracovní době definované v bodě 2.VI), nebo prostřednictvím pracovníka uchazeče vzdálenou správou (po domluvě) nebo prostřednictvím pracovníka uchazeče formou vzdálené konzultace

- součástí instalace a konfigurace provedené uchazečem musí být instalace, konfigurace a zapojení dodaných HW součástí do infrastruktury v požadovaných lokalitách zadavatele (v rámci Frýdku-Místku);

- instalace do Racku,

- připojení k LAN,

- konfigurace management rozhraní,

- nastavení základních reportů a alertů, otestování alertů,

- instalace a konfigurace níže uvedených zařízení a systémů pro zasílání událostí

- 50x Windows server

- 30x Linux server

- 5x databázové systémy

- 35x přepínače HPE (18 stacků)

- 18x AP Aruba

- 2x firewall Fortigate

- antispam Fortimail

- 3x hypervizor VMware

- 2x Brocade FC switche

- zálohovaní Dell DataDomain

- školení administrátorů zadavatele v místě plnění v rozsahu specifikovaném v bodě 2.V). tak, aby byli schopni obsluhovat a spravovat dodané řešení

- 30denní zkušební provoz

- vypracování a předání veškeré dokumentace specifikované v bodě 2.VII).

- předání díla po testovacím provozu za předpokladu odstranění veškerých nedostatků zjištěných během testovacího provozu

1. **Akceptační testy a zkušební provoz**

Součástí akceptačních testů a zkušebního provozu, které navrhne uchazeč, musí být minimálně:

* prokázání kompletnosti dodávky a splnění všech povinných požadavků
* prokázání aktivací aktivačními nebo jinými klíči či prostředky v případě, že je aktivace potřebná
* uchazečem vhodně navržené doplňující testy a kritéria, kterými bude prokázána bezproblémová funkčnost (musí být součástí dokumentu předprojektové analýzy)
* před akceptací a předáním díla proběhne 30denní zkušební provoz. Pokud se vyskytnou během testování nebo zkušebního provozu závady, dodavatel je povinen závady odstranit nejpozději do 8 hodin od nahlášení v pracovní dny v době od 8 hod. do 17 hod.
* v průběhu zkušebního provozu může zadavatel průběžně posílat uchazeči požadavky na úpravy konfigurace, nejpozději však do konce 29. dne zkušebního provozu a uchazeč musí požadované změny realizovat (pokud to je technicky možné)
* dokončením díla se rozumí oboustranné odsouhlasení předávacího protokolu po dokončení testovacího provozu, akceptačních testech a případných úpravách v SW konfiguraci

1. **Školení administrátorů**

Uchazeč zajistí školení zaměstnanců zadavatele v rozsahu minimálně dle následujících požadavků:

* školení pro administrátory zadavatele v rozsahu min. 12 hodin rozdělených do dvou dnů v místě plnění v rozsahu potřebném pro provoz a údržbu systému (ukázka, popis a vysvětlení jednotlivých částí systémů, vysvětlení stávající a tvorby/úpravy nové konfigurace atd.). První část školení proběhne v rámci testovacího provozu, druhá část školení proběhne po dvouměsíčním ostrém provozu sytému.
* školení se dle předpokladu zúčastní 3 zaměstnanci zadavatele (k dispozici je školící místnost s prezentační technikou v místě plnění, popř. vzdálení podle epidemiologické situace)
* náklady na školení musí být zahrnuty v nabídkové ceně jako součást implementace

1. **Harmonogram, plán implementace a odstávek**

Zadavatel vyžaduje dodržení následujícího harmonogramu plnění, jenž začíná v čase T a, v němž jsou uvedeny maximální možné lhůty pro jednotlivé významné milníky této veřejné zakázky. Čas T je definován počátkem platnosti podepsané smlouvy, čili zveřejněním v Registru smluv (zveřejnění smlouvy provádí zadavatel a o zveřejnění informuje uchazeče na email uvedený v kontaktech ve smlouvě). Pokud není dokončen jeden milník, není možno přejít do následujícího.

|  |  |
| --- | --- |
| Předimplementační analýza v místě plnění za přítomnosti zaměstnanců zadavatele z odboru IT a zhotovení projektové dokumentace | T + 15 dní (15 dní) |
| Předání projektové dokumentace zadavateli, připomínkování zadavatelem, zapracování připomínek a předání finální verze k akceptaci zadavatelem | T + 5 dní (20 dní) |
| Dodávka a implementace celého systému | T + 60 dní (80 dní) |
| Zkušební provoz, vypracování dokumentace, školení administrátorů | T + 30 dní (110 dní) |
| Předání díla a dokumentace | T + 1 den (111 dní) |

Bez odstávkové práce mohou probíhat za provozu. Práce, jež omezují provoz nebo vyžadují odstávku, musí být prováděny mimo pracovní dobu. Veškeré práce musí probíhat vždy po domluvě.

Pracovní doba, po kterou je možno pracovat v místě plnění:

• pondělí až pátek od 8:00, dle individuální domluvy je možné od 6:00

• pondělí a středa do 17:00

• úterý a pátek do 13:00

• čtvrtek do 15:00

Odstávky a práce omezující provoz je možno provádět v těchto časech po předchozí domluvě:

• pondělí a středa od 17:30 do 19:00

• úterý a pátek od 14:00 do 19:00

• čtvrtek od 15:30 do 19:00

• odstávky po 19 hod. a o víkendu je možno realizovat dle individuální domluvy

1. **Dokumentace**

Uchazeč po úspěšné instalaci, konfiguraci v době zkušebním provozu vypracuje a dodá zadavateli v písemné podobě podrobné dokumentace (ve formátu DOCX) k nabízenému systému v českém jazyce.

- Provozní dokumentace musí minimálně obsahovat popis a postupy vedoucí k nastavení systému do takového stavu, aby jej bylo možno po instalaci provozovat na základní úrovni. Cílem dokumentu je popsat a zdokumentovat provozní postupy pro zajištění správného, bezchybného a bezpečného provozování nabízeného systému. Rozsah dokumentu bude min. 3 strany. Dokument bude mít formu textového popisu (může být i např. formou okomentovaného config souboru) a bude min. obsahovat:

o konfiguraci sítě (IPv4, IPv6), nastavení připojení a komunikace na další systémy,

o nastavení portů, na kterých služba komunikuje, kam odesílá data, atd.

o nastavení automatických úloh, napojení na LDAP, nastavení systémových účtů atd.

- Technická dokumentace musí obsahovat popis technické specifikace všech klíčových částí/komponent systému, jejich úkol, význam a účel. Popis kompletní aktuální konfigurace, parametrů a nastavení jednotlivých částí systému, tak aby je bylo možno nadále provozovat a spravovat. Cílem dokumentu je popsat a zdokumentovat technickou stránku a aktuální konfiguraci systému. Rozsah dokumentu bude min. 10 stran. Dokument bude mít formu textového popisu a může být doplněn obrazovým návodem.

- Veškerá dokumentace a příručky se po předání zadavateli stávají jeho majetkem a může s nimi nakládat dle svých potřeb.