SPRÁVA ŽELEZNIC

Naše zn. 72742/2023-SŽ-GŘ-O8

Věc: Vysvětlení zadávací dokumentace č. 1

Sektorová nadlimitní veřejná zakázka na dodávky s názvem:

„**Log management a SIEM**"

Správa železnic, státní organizace (dále jen „Zadavatel") obdržela dne 20. 10. 2023 v 10:47 hodin žádost o vysvětlení zadávací dokumentace. Zadavatel formou Vysvětlení zadávací dokumentace odpovídá na tuto žádost doručenou k veřejné zakázce následovně:

Dotaz č. 1:

Dotaz k bodu ID 10 - Příloha č. 20 - Log management a SIEM dotazník

Námi nabízené řešení se dodává jako Vmware image. Bude Zadavatel toto akceptovat?

Odpověď:

Ano, takový způsob dodání je jeden z možných, který je v souladu s požadavkem ID:10 Zadavatele. Samozřejmě je nezbytné, aby byly podporovány i další uvedené typy operačních systémů, pokud v rámci platformy sběru logů bude řešení vyžadovat na takové systémy instalovat své komponenty.

Dotaz č. 2:

Dotaz k bodu ID 30 - Příloha č. 20 - Log management a SIEM dotazník

Nabízené řešení může být komplexní, kdy požadavek na kompletní správu je velmi nestandartní. Bez detailního popisu požadavků pro automatizaci by vést k neporovnatelným nabídkám. Chápe uchazeč, že požadavek na automatizaci je z důvodu primárně automatizace přidávání a konfigurace zdrojů logů, případně zakazování a povolování pravidel. V případě, že námi nabízené řešení podporuje automatizaci minimálně výše uvedených požadavků, bude takovéto námi nabízené řešení akceptovatelné?

Odpověď:

Zadavatel si komplexnost poptávaného řešení plně uvědomuje, a právě z tohoto důvodu vyžaduje, aby jednotlivé komponenty řešení bylo možné spravovat pomocí automatizačních nástrojů. Kompletní správa řešení pomocí automatizačních nástrojů znamená, že automatizace musí být možná minimálně pro konfigurace příjmu logů z nových zdrojů, ovládání detekčních pravidel a správu konfigurací jednotlivých komponent dodávaného řešení Log management a SIEM.

Správa železnic, státní organizace
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A 48384

Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČ: 709 94 234 DIČ: CZ 709 94 234
www.spravazeleznic.cz

Dotaz č. 3:

Dotaz k bodu ID 40 - Příloha č. 20 - Log management a SIEM dotazník

Uchazeč konstatuje že MapReduce je obecný přístup, který má za cíl paralyzovat vyhledávání v datech. Bude Zadavatel akceptovat řešení využívající obecné principy paralelizace hledání v datech?

Odpověď:

Zadavatel požaduje, aby řešení umožňovalo procesy paralelního zpracování dat při vyhledávání, a právě proto použil pro definici tohoto požadavku obecně používaný termín MapReduce. Zadavatel tedy bude akceptovat řešení využívající obecné principy paralelizace hledání v datech.

Dotaz č. 4:

Dotaz k bodu ID 43 - Příloha č. 20 - Log management a SIEM dotazník

Technická specifikace (Příloha č.1 ZD, bod 2.4.3) uvádí jako možnosti nasazení clusteru active x standby.

Active – standy cluster je dostačují pro zajištění redundance a vysoké dostupnosti SIEM řešení. Bude Zadavatel akceptovat řešení s clusterem active x standby?

Odpověď:

Zadavatel bude akceptovat dodávku řešení, které bude provozováno minimálně v režimu vysoké dostupnosti Active – Standby (jak specifikuje kapitola 2.4.3 Přílohy č. 1 - Technická specifikace), ale vyžaduje, aby nabízené řešení podporovalo také režim Active – Active, jak uvádí ID 43 - Přílohy č. 20 - Log management a SIEM dotazník.

Dotaz č. 5:

Dotaz k bodu ID 46 - Příloha č. 20 - Log management a SIEM dotazník

Z požadavků na platformu (je nabízena virtualizace) a dalších požadavků Zadavatele neplyne nutnost provozovat celé řešení v kontejnerech. Bude Zadavatel akceptovat řešení postavené na virtuálních image využívajících platformu Zadavatele?

Odpověď:

Ano, řešení postavené na virtuálních image pro platformu Zadavatele je možné. Zadavatel však požaduje, aby nabízené řešení podporovalo provoz jednotlivých komponent v kontejnerových platformách, přestože aktuální nabízená virtualizační platforma, resp. její aktuálně definované služby takovou nabídku neuvádí, a to z důvodu plánovaného rozvoje HW platformy.

Dotaz č. 6:

Dotaz k bodu ID 109 - Příloha č. 20 - Log management a SIEM dotazník

SIEM obecně neprovádí deep packet inspection kde by tento požadavek mohl být relevantní. Uchazeč prosí o zvážení vyjmutí tohoto požadavku, jelikož je diskriminační.

Odpověď:

Bod ID 109 Přílohy č. 20 - Log management a SIEM dotazník uvádí požadavek: *"Možnost volitelného „vzorkování" – rychlejší prezentace výsledků zobrazením každého n-tého paketu".* Není tedy uvedeno, že by řešení mělo podporovat hloubkovou inspekci paketů. Zadavatel pouze požaduje, aby v případě jeho zájmu o přímý sběr informací o síťovém provozu do platformy Log management a SIEM, byla podporována možnost vzorkování provozu. Funkce vzorkování může být poskytnuta v rámci jakékoli komponenty nabízeného řešení.

Dotaz č. 7:

Dotaz k bodu 2.4.5 Architektura uložišť z Příloha č. 1 - Zadávací dokumentace (technická specifikace)

Uchazeč nerozumí plně tomuto požadavku s ohledem na tabulku „Požadavky na službu Platformy", kde je uvedeno pouze jedno uložiště hot/warm se stejnou hodnotou IOPS. Tedy mezi uložišti není rozdíl.

Očekává Zadavatel rozdělení uložiště na hot a warm v rámci dodávky. Tedy zmiňované 3 měsíce hot a 15 měsíců na warm? Námi nabízené řešení toto umožňuje.

Nicméně, z pohledu architektury námi nabízeného řešení se jedná o zásadní rozdíl s dopadem na požadované zdroje a v případě, že není mezi uložišti rozdíl, tak nedává smysl stavět architekturu v rámci dodávky dle tohoto požadavku. Bude Zadavatel akceptovat architekturu řešení využívající dva tiery tedy hot/warm (online data) a cold (archiv)?

Mohl by Zadavatel zároveň poskytnout příklad vyplněné tabulky Příloha č. 19 - Požadavky na služby Platformy?

Odpověď:

Bod 2.4.5 Přílohy č. 1 - Zadávací dokumentace (technická specifikace) uvádí: *"Systém Log management musí podporovat rozklad diskové kapacity na různá úložiště s různou úrovní přístupnosti a rychlosti, která jsou známa jako úložiště HOT, WARM a COLD. (…) SŽ vyžaduje, aby nabízené řešení umožňovalo na aplikační úrovni rozlišování druhů úložišť pro: HOT úložiště, která jsou specifická tím, že jejich stáří od doby uložení do Log management není delší než 3 měsíce WARM úložiště budou všechna ostatní data až do požadovaného období pro uložení 18 měsíců. Využití úložiště úrovně COLD bude sloužit pouze pro účely archivace."*
Příloha č. 19 - Požadavky na služby Platformy uvádí požadavky na HW platformu Zadavatele, přičemž aktuálně úrovně HOT a WARM nerozlišuje.
Zadavatel tedy bude akceptovat architekturu řešení, která bude využívat jen dvě úrovně (tiery) HOT/WARM a COLD. Zadavatel však s ohledem na plánovaný rozvoj HW platformy požaduje (jak uvádí v Technické specifikaci), aby nabízené řešení umožňovalo na své aplikační úrovni rozlišovat také mezi úrovněmi HOT a WARM. Dodavatel nebude muset rozlišení na HOT, WARM a COLD uložiště (tedy všechny tři úrovně) jeho řešení při návrhu architektury využít, když HW platforma Zadavatele aktuálně úrovně HOT a WARM nerozlišuje.

Zadavatel připravil ukázku možného vyplnění požadavků na služby Platformy SŽ a umístil ji na listu „Příklad" přílohy č. 19 – Požadavky na služby Platformy SŽ, která je součástí zadávací dokumentace.

Závěr

Zadavatel setrval na zadávacích podmínkách a jeho vysvětlení zcela odpovídá původnímu znění zadávací dokumentace. Neprovedl tak žádnou změnu zadávací dokumentace, jež by vyžadovala prodloužení lhůty pro podání nabídek, nicméně z důvodu nedodržení zákonné lhůty pro uveřejnění odpovědi na žádost o vysvětlení zadávací dokumentace, přistoupil Zadavatel

k prodloužení lhůty pro podání nabídek, jež odpovídá době, o kterou nebyla lhůta pro vypořádání žádosti o vysvětlení dodržena, tedy jeden pracovní den. Lhůta pro podání nabídek je tak nově stanovena na den 7. 11. 2023 do 8:30 hodin.

Ing. Dalibor Fajkus
26.10.2023 13:56
Podepsáno elektronicky

……

Ing. Dalibor Fajkus
náměstek ředitele organizační jednotky pro rozvoj