DÍLČÍ OBJEDNÁVKA č. 10

Číslo související Rámcové dohody: 01IN-005282
Číslo dílčí objednávky: 01IN-005553
Ze dne: 28.6. 2023

Objednatel:
Ředitelství silnic a dálnic ČR
Úsek informatiky
Čerčanská 2023/12, 140 00 Praha 4
IČO: 65993390
DIČ: CZ65993390

Dodavatel:
IBA CZ, s.r.o.
Radlická 751/113e, 158 00 Praha 5
IČO: 25783572
DIČ: CZ25783572

Tato dílčí objednávka je návrhem na uzavření dílčí smlouvy ve smyslu čl. III uzavřené Rámcové dohody. Způsob akceptace dílčí objednávky dodavatelem (uzavření dílčí smlouvy), obchodní, smluvní a platební podmínky a další práva a povinnosti smluvních stran touto dílčí dohodou výslovně neupravená stanovuje Rámcová dohoda.

Na základě uzavřené Rámcové dohody u Vás objednáváme:

Služby dle nabídky, která je přílohou č. 1 této dílčí objednávky.

Místo dodání: ŘSD ČR, Čerčanská 2023/12, 140 00 Praha 4;

Termín dodání: do konce 9/2023 od nabytí účinnosti objednávky;

Kontaktní osoba objednatele: [redacted]

Celková hodnota objednávky v Kč bez DPH / vč. DPH: 658.400,- Kč / 796.664,- Kč

Jméno a příjmení oprávněné osoby objednatele: [redacted]

Přílohy:
Příloha č. 1_ŘSD_Návrh řešení- IDM_HA_Jump

PODEPSÁNO PROSTŘEDNICTVÍM UZNÁVANÉHO ELEKTRONICKÉHO PODPISU DLE ZÁKONA Č. 297/2016 SB., O SLUŽBÁCH VYTVÁŘEJÍCÍCH DŮVĚRU PRO ELEKTRONICKÉ TRANSAKCE, VE ZNĚNÍ POZDĚJŠÍCH PŘEDPISŮ

Příloha č. 1

Návrh řešení – midPoint v režimu vysoké dostupnosti (HA) a napojení na JumpHost

Pro společnost:

Ředitelství silnic a dálnic ČR

Datum: 21. června 2023

IBA CZ, s. r. o.,
Radlická 751/113e,
158 00 Praha 5

IČO: 25783572
DIČ: CZ25783572

www.ibacz.eu
info@ibacz.eu
(+420) 251 050 100

OBSAH

1 POPIS POŽADAVKU

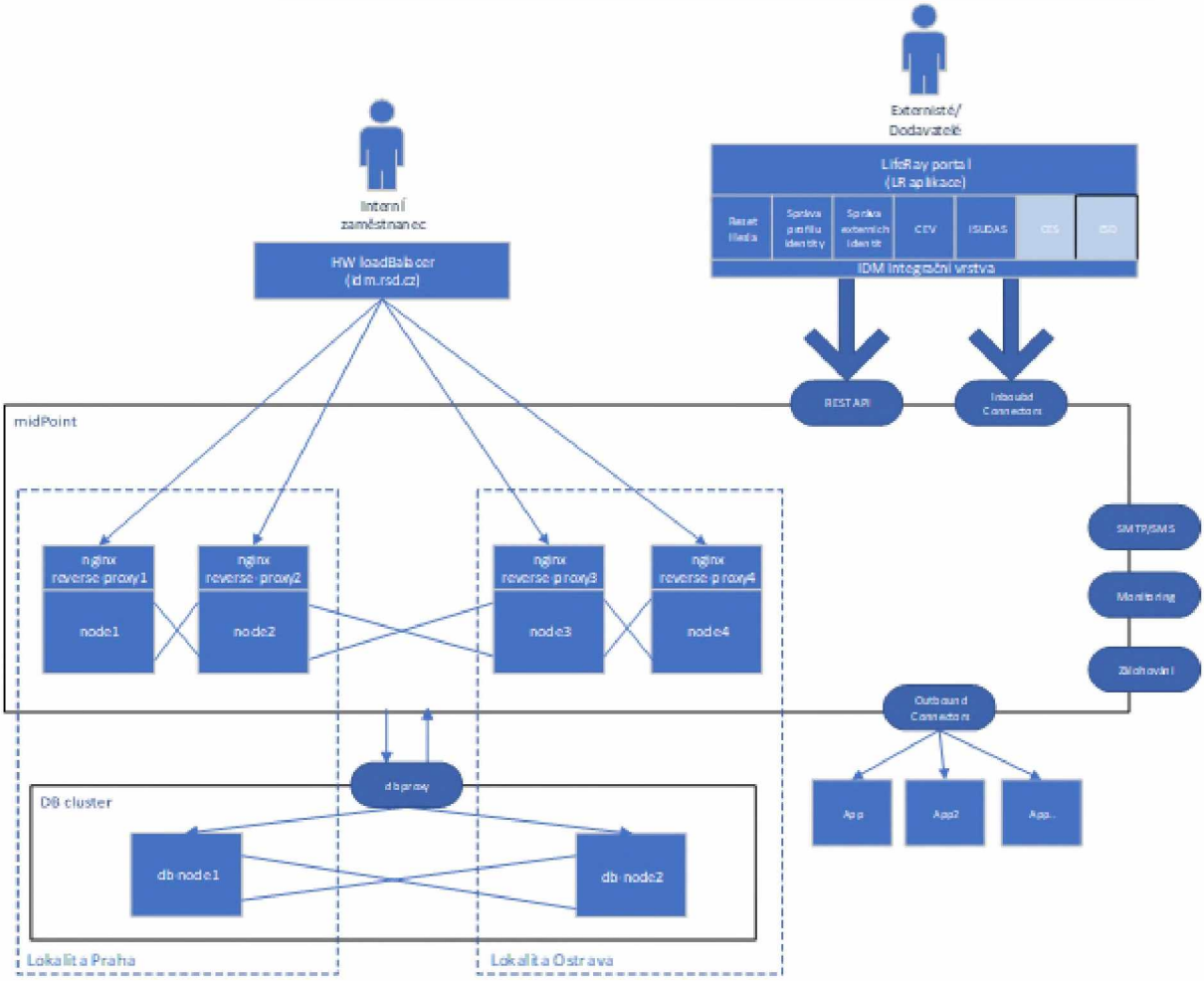
Táto nabídka je vytvořena na základě požadavků společnosti ŘSD ohledně Identity Managementu a vysoké dostupnosti midPoint. Zároveň na základě poptávky po napojení IDM na JumpHost a následného řízení přístupových oprávnění.

1.1 Midpoint v režimu vysoké dostupnosti (HA)

MidPoint, jakožto webovou aplikaci je možné provozovat kromě stand-alone řešení rovněž jako řešení ve vysoké dostupnosti. Z pohledu architektury je možné aplikaci horizontálně škálovat, přičemž jednotlivé nody řešení je možné využít a rozdělit pro různé typy operací.

Princip vysoké dostupnosti spočívá ve vytvoření jednoho společného perzistentního úložiště, kde jednotlivé aplikační nody přistupují a sdílejí si vzájemně data.

Jednotlivé nody je pak možné nakonfigurovat tak, aby každý jednotlivý node byl určen k vykonávaní jiného typu úloh. Typicky je např. možné využít 2 samostatné nody (node1 a node3) jako prezentační vrstvu – kam přistupují identity přes uživatelskou samoobsluhu, včetně přístupu aplikací třetích stran přes REST API pro vyřízení jejich požadavků do vlastní aplikace (např. aplikace pro Reset Hesla), ostatní node (node2 a node4) je možné využít na zpracování a obsluhu pravidelně běžících úloh, které běží pravidelně na pozadí.



Obrázek 1 midPoint HA (active-active)

Aby bylo řešení dostatečně robustné a stabilní je nutné kromě zabezpečení vysoké dostupnosti aplikační vrstvy, zvážit vysokou dostupnost i pro samotnou databázi (před samotným rozhodnutím, doporučujeme udělat performance monitoring DB, podívat se na její týdenní/měsíční vytížení, případně navýšení systémových prostředků a tunning). V rámci své infrastruktury provozuje ŘSD dvě samostatná datacentra (Praha/Ostrava) propojena 100Mbit linkou. High-level návrh předpokládá s rozložením infrastruktury do obou datacenter v režimu Active-Active.

Přístup pro privilegované účty správců aplikace midPoint, doporučujeme zabezpečit prostřednictvím 2FA autentizace. Vhodnou platformou poskytující tyto služby je např. Microsoft Authenticator. Pro integraci na tuto službu je možné využít protokol OIDC který midPoint nativně podporuje.

Přihlašování jednotlivých správců (přes privilegovaný účet) navrhujeme řešit vystavením samostatného endpoint pro tento účel. V rámci přihlašovacího procesu bude rovněž vykonaná dodatečná autorizace identity, na přirazení role „Správce systému". V případě že přihlašovaný uživatel nebude mít roli přirazenou, systém odmítne vykonat přihlášení a uživateli zobrazí chybovou správu.

1.2 Napojení na JumpHost

Z pohledu systému midPoint se jedná o integraci nové aplikace a řízení přístupových oprávnění. Pro integraci JumpHost s prostředím midPoint je možné využít standardního konektoru již využívaného pro řízení přístupů Active Directory.

Prerekvizitou na napojení IDM na JumpHost je vydefinování a vyplnění Setup Formu pro integraci. Pro naplnění prerekvizity ŘSD poskytneme součinnost. Součástí Setup Form jsou informace jako:

- Definice typů uživatelských účtů.
- Definice uživatelských atributů.
- Definice pravidel pro naplňování atributů.
- RBAC matice – definice přístupových oprávnění – skupin.
- Jmenná konvence.
- Konvence pro definici hesel.
- Příprava integrační dokumentace – setup form jumpHost AD.

Nutné technické prerekvizity pro napojení za stranu ŘSD:

- Vytvoření technického uživatele pro přístup k jumpHost AD.
- Nastavení oprávnění pro technického uživatele.
- Nastavení prostupů – midPoint> jumpHost AD (636).
- Nastavení zabezpečeného připojení (ldaps).

2 SOUČINNOST

V rámci analytické fáze požadujeme součinnost zaměstnanců RSD (případně dodavatelů systému) v roli:

Projektový manažér0

Zastřešuje koordinaci činností, realizaci integračních požadavků analýzy anebo implementace na straně zákazníka.

Garant systému (byznys vlastník):

V rámci analýzy poskytuje konzultace v rozsahu dotčených systém, u kterých se požaduje ukládání a verzování zdrojových kódů.

Garant (-i) (Integrační architekt, vlastník služby. vlastník oblasti. apod.):

Zaměstnanec je garantem projektu v oblasti architektury řešení. V průběhu projektu je obeznámen s možnými variantami použité technologie, kdy zabezpečí a odsouhlasí, že navržené řešení lze implementovat do existujícího prostředí.

Součinnost při analýze

Pro úspěšné dokončení analytické fáze je nutná součinnost zákazníka v rozsahu potřebném pro zafixování potřeb, integrací a oblastí služeb.

3 HARMONOGRAM

Termín realizace veškerých úprav je do konce 09/2023.

4 CENA

4.1 Nabídková cena

Předpokládaná, maximální cena realizace je **658 400 Kč bez DPH.**

	Položka (role, příp. skupina rolí)	M.J.	Počet M.J.	Cena za 1 M.J. v Kč bez DPH	Cena za počet M.J. v Kč bez DPH
ŘSD	konzultant/ analytik	MD	16,00	[redacted]	[redacted]
	projektových manažer	MD	15,00	[redacted]	[redacted]
	architekt/ návrhář	MD	8,00	[redacted]	[redacted]
	programátor/kodér	MD	69,00	[redacted]	[redacted]
	specialista (L2, L3 podpory, release, technical writer, apod.)	MD	17,00	[redacted]	[redacted]
	Celkem		**125,00**	**Cena celkem**	**658 400,00 Kč**

4.2 Fakturační milníky

Fakturace bude probíhat na základě potvrzených akceptačních protokolů ze strany ŘSD.

[redacted]

Digitálně podepsal [redacted]
Datum: 2023.06.29 09:31:10 +02'00'

Digitálně podepsal: [redacted]
Datum: 29.06.2023 8:50:00 +02:00