Příloha č. 5 – Technická specifikace

Předmět veřejné zakázky

Předmětem rámcové dohody je povinnost poskytovatele zajistit provoz virtualizované HW infrastruktury (Infrastructure as a Service – IaaS) pro jednotlivé internetové projekty Nových médií podle aktuální potřeby (integrační část projektu mujRozhlas - rAPI, web mujRozhlas.cz, web Ježíškova vnoučata, informace o programu atp.). Zároveň půjde o infrastrukturu použitelnou i pro případný provoz záložního webu ČRo.

Cloudová infrastruktura, která je předmětem rámcové dohody, se nesmí nacházet v datovém centru, kde je umístěn aplikační cloud, viz článek IV. odst. 3. rámcové dohody, a to na adrese: Kodaňská 1441/46, 101 00 Praha.

1. Požadované technické parametry služby

parametr	**hodnota**
specifikace služby	managed server hosting
cloudová technologie (hypervisor)	VMware vCloud Director min. verze 9.7
počet VM / vAPPs	128 / 32
počet vCPU x frekvence (GHz)	128 x 2,6
vRAM (GB)	512
velikost úložiště (TB)	100
výkon úložiště dle účelu	standardní / vysoký / špičkový
Síť mezi VM	min. 1 Gbit/s
Konektivita	vyhrazená linka 1 GBit/s
veřejné statické IPv4 adresy (počet)	12
veřejné statické IPv6 adresy (počet)	Segment /56
úroveň provozní bezpečnosti datového centra	TIER 3
zálohování	Automatizované zálohování shapshotů (Veeam)

2. Cloudová technologie

Objednatel požaduje cloudovou technologii VMware vCloud Director minimálně ve verzi 9.7. Nižší verze objednavatel nepřipouští z důvodu podpory HTML5 Tenant Portal Enhancements, Terraform Provider 2.0 a podpory kontejnerových služeb jako je Container Service Extension (CSE) 1.2s.
Objednatel požaduje konkrétně technologii VMware vCloud s ohledem na skutečnost, že interní zaměstnanci nebo externí smluvní partneři jsou znalí práce s požadovanými technologiemi a jejich změna by znamenala nákladné přebudování a úpravy stávajících postupů.

3. Požadavky na datové centrum

3.1. Provozní bezpečnost

Za účelem garance vysoké dostupnosti služeb datového centra objednatel požaduje, aby datové centrum dosahovalo provozní bezpečnosti minimálně úrovně TIER III ve všech parametrech dle klasifikace Uptime Institute. Naplnění tohoto požadavku musí být prokázáno jedním z níže uvedených způsobů:

a) doložením certifikátu od Uptime Institute alespoň na úrovni návrhu datového centra, tzv. "Certification of Design Documents"
b) čestným prohlášením poskytovatele

Pokud se prokáže, že některý z parametrů datové centra nedosahuje úrovně TIER III dle klasifikace Uptime Institute má objednatel právo uplatnit sankce viz článek XIV. odst. 8 rámcové dohody.

3.2. Dostupnost

Dostupnost služeb datového centra musí dosahovat alespoň 99,98% ročně (dle klasifikace TIER III).

4. Úložiště

Cloudové úložiště bude poskytovat 3 výkonové úrovně dle účelu jeho využití.

Úroveň výkonu	**rychlost čtení / zápisu**	**Účel úložiště**
standardní	rychlost čtení / zápisu není prioritou	zálohování a archivace dat
vysoká	vysoká rychlost čtení / zápisu	běžné aplikace a databáze
špičková	špičková rychlost čtení a zápisu dat	databáze s min. dobou odezvy (business critical)

5. Zálohování

Poskytovatel bude automaticky vytvářet snapshoty běžících VM pomocí technologie Veeam a zálohovat je tak, aby mohl tyto zálohy použít i objednavatel pro obnovu VM mimo infrastrukturu poskytovatele, především pak na prostředcích objednatele. Vzhledem k tomu, že objednatel již disponuje zálohovací technologií společnosti Veeam a virtualizační infrastrukturou VMware vSphere, počítají jeho havarijní plány a plány obnovy s případnou možností přemístění VM na tuto infrastrukturu.

6. Konektivita

- Minimálně 2 nezávislé optické trasy konektivity
- Přímá konektivita do NIX
- Neomezený datový přenos v rámci ČR i mimo ČR.
- Konektivita minimálně 1 Gbps.

7. Administrační rozhraní

Služba musí poskytnout zabezpečený přístup do administračního rozhraní pomocí webového prohlížeče (bez nutnosti využívat FLASH technologii) a umožňovat následující administraci - vytváření virtuálních strojů, konfigurace jejich parametrů, nastavování sítě, poskytovat přehled o přidělování systémových prostředků, zálohování.

8. API

Služba musí umožňovat plnohodnotnou správu, konfiguraci a vytváření VM skrze vCloud Director API nebo kompatibilní.

9. Dokumentace

9.1. Veškerá níže zmíněná dokumentace je v češtině nebo angličtině.
9.2. Správnost a úplnost dokumentace je kontrolována a aktualizována každé 3 měsíce.
9.3. Kompletní uživatelská i správcovská dokumentace všech komponent, které jsou součástí řešení
9.4. Dokumentace k zabezpečení a procesům (např. VPN, ukládání hesel, TLS atd.) zejména pro účely auditů a kontrol třetích stran.

10. Podpora a údržba

10.1. Poskytovatel provozuje online Helpdesk - elektronickou evidenci všech Požadavků, reakcí na ně a jejich způsobů vyřešení. Všechna data z Helpdesku jsou k dispozici po celou dobu trvání Smlouvy. V evidenci jsou vedeny informace o tom, kdy byl vznesen Požadavek, kdo jej vznesl, jaký byl jeho obsah, kdo jej vyřizoval, kdy bylo na Požadavek reagováno a kdy, jak byl Požadavek vyřešen a jak dlouho trvalo jeho řešení. Provoz Helpdesku zajištěn v režimu 24/7, uchovávání historie požadavků po celou dobu trvání Smlouvy.
10.2. Objednatel má k dispozici telefonní hotline v režimu 24 hodin / 7 dnů v týdnu.
10.3. Servisní doba Poskytovatele je 365 dní v roce, 7 dní v týdnu, 24 hodin denně.
10.4. Pro servisní práce a údržbu infrastruktury může Poskytovatel využít plánované odstávky (tzv. Servisní okno) v maximálním rozsahu 2 hodiny v součtu za kalendářní měsíc. Ve výjimečných případech (např. jednorázová migrace apod.) lze domluvit se souhlasem Objednatele i servisní okno delší.
10.5. Poskytovatel je povinen písemně informovat Objednatele o plánované odstávce v dostatečném předstihu, minimálně 14 kalendářních dní.
10.6. Minimální dostupnost infrastruktury je 99.9 % v každém kalendářním měsíci.
10.7. Nedostupnost je zjištěna monitorovacím nástrojem Poskytovatele, nebo též může být nahlášena při jejím zjištění Objednatelem.
10.8. Dostupnost infrastruktury v procentech se vypočítá za každý kalendářní měsíc tak, že celkový počet celých minut, po který byla infrastruktura dostupná nebo probíhala plánovaná údržba v servisním okně, se vydělí celkovým počtem minut v měsíci a vynásobí 100. Pokud je mezi samostatnými nedostupnostmi období kratší než 10 minut, považuje se toto celé období za nedostupnost.
10.9. Je dodržována reakční lhůta (fyzickým člověkem, ne automatem) a lhůta pro odstranění vady od nahlášení závady dle následující tabulky:

Stupeň priority závady	*Popis závady*	*Reakční lhůta od oznámení požadavku*	*Lhůta pro odstranění vady od oznámení požadavku*
1- Kritický incident	Infrastruktura není dostupná žádným způsobem	1 hodina	4 hodiny

2 - Vážný incident	Je dostupná administrace infrastruktury, ale vyskytují se vážné výkonnostní problémy	4 hodiny	24 hodin
3 - Běžný incident	Vyskytuje se problém, který ale významně nesnižuje výkon ani dostupnost infrastruktury	1 pracovní den	3 pracovní dny
4 - Běžný požadavek	např. úprava konfigurace nebo drobná chyba, která neovlivňuje činnost	2 pracovní dny	5 pracovních dnů

10.10. Do 5. dne každého měsíce je Objednateli zaslán report, který obsahuje:
- 10.10.1. Dostupnost služby
- 10.10.2. Přehled využitých servisních oken
- 10.10.3. Přehled řešených Incidentů s výsledným stavem
- 10.10.4. Využití kapacity

10.11. V případě, že nějaká v infrastruktuře použitá součást obsahuje bezpečnostní chybu, je součást aktualizována nejpozději do 30 kalendářních dnů, pokud je splněno že má chyba přidělený CVE identifikátor a současně existuje opravná verze či workaround od Poskytovatele či autora této součásti.

10.12. Je veden záznam o servisních zásazích na Infrastruktuře s přesnými záznamy času, pracovníků podílejících se na zásahu a popis provedené operace.

10.13. Neexistují společné přístupové účty, každý pracovník Poskytovatele má samostatný přístup vedený na jeho jméno.

10.14. V případě ukončení poskytování služby poskytne poskytovatel objednateli součinnost při migraci na jinou infrastrukturu.

10.15. Součinností při migraci na jinou infrastrukturu je myšleno poskytnutí odborného školení zaměstnancům Objednatele, na provoz v rozsahu 3 (tří) pracovních dnů v budově Objednatele. Cena tohoto školení byla Poskytovatelem zahrnuta v ceně úvodní migrace (viz. Příloha – Cenová nabídka poskytovatele). Na školení Poskytovatel Objednateli zejména:

A. popíše obsah veškeré písemné dokumentace, vzniklé v souvislosti s plněním Smlouvy, která byla nebo má být předána Objednateli, a vysvětlí, k čemu dokumentace slouží a jak s ní dále pracovat;
B. předá přístupy k Infrastruktuře, včetně všech přístupových údajů, hesel a bezpečnostních kódů a přístup do všech administrátorských rozhraní a vysvětlí, k čemu slouží a jaké mají funkce;

11. Milníky

1. dodání virtualizované HW infrastruktury připravené pro migraci stávající infrastruktury, migraci dat a testování – **nejpozději do 2 týdnů od účinnosti 1. dílčí smlouvy**;

2. dokončení migrace stávající infrastruktury a uvedení cloudu do plného provozu – **4 týdny od účinnosti 1. dílčí smlouvy**.

12. Migrace

Objednatel požaduje provedení migrace stávající infrastruktury bez dopadu na služby objednatele provozované v současné infrastruktuře. Za tímto účelem je poskytovatel povinen koncipovat migraci jako bezvýpadkovou.
Pokud nebude možné z technických důvodů dosáhnout úplné bezvýpadkovosti, je povinnen poskytovatel zajistit minimalizaci výpadků, tak aby v celkovém součtu nepřesáhly 2 hodiny v časovém okně definovaném objednatelem (např. mezi půlnocí a 4 hodinou ranní). Dle potřeb objednatele může být migrace rozdělena na více takových oken (každé s výpadky v součtu pod 2 hodiny). Celkový čas výpadků přes všechna migrační okna nesmí překročit 4 hodiny. Objednatel pro tento účel poskytne nezbytně nutnou součinnost.

13. Současný technický stav

Platforma je tvořena několika desítkami (více než padesát) virtuálních strojů (dále len VM) seskupených do několika logicky uspořádaných skupin (dále jen vApp).

Jako OS je použit Debian ve verzích 7-10, případně Ubuntu LTS.

Použitý middleware zahrnuje širokou škálu běžně používaných technologií. V naprosté většině se jedná o otevřený software, například:

- HAproxy
- Varnish
- Nginx
- MariaDB / Galera
- Elastic Stack
- Redis
- RabbitMQ
- Zabbix
- Cassandra
- Minio
- Flask
- Zabbix
- Kong

Jediným zástupcem komerčního software je několik instancí Wowza Streaming Engine.

Architektura jednotlivých vApps se obecně snaží poskytovat vysokou dostupnost a horizontální rozkládání zátěže (HA/LB řešení), vždy v rámci možností použitých technologií. Pokud je to vhodné, je použitý clustering (Galera, Elasticsearch, Kong, Cassandra).

Monitoring všech VM zajišťuje nástroj Zabbix s vhodně nastaveným alertingem.

Na aplikační úrovni se opět jedná o běžné technologie, například:

- PHP / Symfony
- Drupal
- Python / Celery
- Bash