Příloha č. 5 – Technická specifikace

Předmět, účel zakázky a popis dnešního stavu

Předmět veřejné zakázky

Předmětem veřejné zakázky je zajištění služby provozu specializovaného aplikačního cloudu pro redakční systém Drupal a případné další internetové aplikace ČRo. Součástí služby je poskytnutí HW infrastruktury dimenzované a optimalizované na požadovaný provoz aplikací, administrace této infrastruktury, správa nezbytného SW prostředí, zajištění konektivity do internetové sítě, nastavení SLA pro nepřetržitý provoz a zajištění bezpečnosti, podpory a údržby aplikačního cloudu.

Popis dnešního stavu

Internetové pilíře Rozhlas.cz a iROZHLAS.cz Českého rozhlasu (ČRo) jsou provozovány a rozvíjeny na vlastním řešení koncipovaném na platformě Drupal 7. Jedná se zejména o weby:

- irozhlas.cz
- Weby celoplošných stanic: radiozurnal.rozhlas.cz, wave.rozhlas.cz,...
- Weby regionálních stanic: brno.rozhlas.cz, olomouc.rozhlas.cz,...
- Projektové weby: 1968.rozhlas.cz a další

Celkem jde zhruba o 60 webů na jedné instanci drupalu (sdílejí databázi a administraci), které jsou umístěny v cloudu současného poskytovatele. Bližší a technické informace k aktuálnímu stavu jsou rozepsány v příloze *Současný technický stav.*

Obecně k předmětu veřejné zakázky

Předmětem veřejné zakázky je správa a rozvoj infrastruktury na provoz webů ČRo, tak aby tato infrastruktura a model spolupráce s jejím poskytovatelem reflektovala aktuální požadavky Objednatele. Zejména záleží na provozní nezávislosti webů, rychlém publikování nových funkcí na produkční prostředí a jasném přehledu o chování systému za účelem jeho další optimalizace. Toto vše při zachování vysoké dostupnosti a spolehlivosti stávající infrastruktury po dobu minimálně tří let. Předpoklad zvýšení zátěže v budoucnu je dále rozepsaný v příloze *Odhad nárustu zátěže infrastruktury.*

Účel veřejné zakázky

S ohledem na výše nastíněný výchozí stav a možnosti, které se Objednateli v souvislosti s Veřejnou zakázkou nabízí, vymezil Objednatel v následujících bodech Účel veřejné zakázky:

1. Vzhledem k termínu ukončení smlouvy se stávajícím Poskytovatelem a veřejnému zájmu využívat prostředí co nejdříve má Objednatel zásadní zájem na dodržení harmonogramu plnění.
2. Infrastruktura musí bez poklesu výkonu a spolehlivosti obsloužit stávající zátěž a dále zachovat výkon a spolehlivost po dobu minimálně 36 měsíců.
3. Infrastruktura musí být koncipována tak, aby přetížení jedné části / webu nezpůsobilo nedostupnost dalších částí / webů.
4. Stávající stav a možnosti infrastruktury musí být zlepšeny v oblastech:
    1. Odbavování audií je co nejvíc nezávislé na odbavování požadavků Drupalem
    2. Pro deployování mít možnost využít CD via Deployer v BitBucket pipelines
    3. Bezpečnost

Minimální požadavky na řešení a službu aplikačního cloudu

Následující kapitoly shrnují minimální technické i netechnické požadavky objednatele na poptávané řešení aplikačního cloudu a s tím spojené služby dodavatele. Dodavatel se zavazuje splnit níže specifikované požadavky dle harmonogramu uvedeném v kapitole *Milníky.*

Součástí řešení nejsou

- DNS servery - spravuje Český rozhlas, úpravy DNS záznamů podléhají schválení.
- SMTP servery - spravuje Český rozhlas, infrastruktura se k nim pouze bude připojovat.

1. Technické požadavky na produkční infrastrukturu

1.1. Požadavky na výkon

1.1.1. Řešení obslouží zátěž současné infrastruktury bez poklesu rychlosti - viz příloha *Současný technický stav.*

1.1.2. Řešení je rozděleno na tři hlavní části (irozhlas.cz, *.rozhlas.cz a administrace) - přetížení vyvolané jednou z nich nesmí způsobit nedostupnost jiné části.

1.1.3. Pro odbavování audií je využita separátní doména (např. audio.rozhlas.cz) s vlastním LB

1.1.4. Oddělení na úrovni LB či Proxy Cache - provoz přihlášených uživatelů/editorů (identifikace dle konkrétního cookie) bude vždy končit na webserverech. Provoz irozhlas.cz, případně *.rozhlas.cz může být v případě potřeby od webserverů úplně odstřižen, servírovaný bude jen obsah z Proxy Cache.

1.2. Požadavky na datacentrum a zapojení serverů

1.2.1. Dostupnost služeb datacentra alespoň 99.95% ročně

1.2.2. Garantováno minimálně 72 hodin provozu při výpadku el. energie
1.2.3. Minimálně 2 dieselgenerátory
1.2.4. Redundance všech komponent alespoň N+1
1.2.5. Redundantní chlazení
1.2.6. Protipožární systém, automatický hasící systém
1.2.7. Přístup na datový sál pomocí dvou faktorů (čip / biometrika, čip / PIN, klíč / pin, …)
1.2.8. Kamerový systém s uchováváním záznamů
1.2.9. K infrastruktuře nemají přístup jiné osoby, než pověřené Dodavatelem
1.2.10. Minimálně 2 nezávislé optické trasy konektivity
1.2.11. Přímá konektivita do NIX
1.2.12. Neomezený datový přenos v rámci ČR i mimo ČR.
1.2.13. Konektivita minimálně 5 Gbps bez ohledu na použitou trasu.
1.2.14. Použito IPv4 i IPv6.
1.2.15. Servery a síťové prvky propojeny vyhrazenou LAN 10 Gbps
1.2.16. Celá infrastruktura a procesy dodavatele jsou připraveny na to, že objednatel může potřebovat předřadit celému řešení jednu popř. více proxy (ať už od dodavatele, svoje či třetí strany).
1.2.16.1. Nasazení takovýchto proxy je možné zvlášť pro testovací i produkční prostředí.
1.2.16.2. Dodavatel upraví konfigurace do 30 dnů po sdělení objednatele, že má v plánu takové řešení nasadit. Objednatel sdělí dodavateli IP adresy nebo URL kde jsou k dispozici IP adresy těchto proxy a jak často je třeba seznam aktualizovat.
1.2.16.3. Před faktickou aktivací proxy (typicky změnou DNS záznamů) objednatel informuje o přesném datu a času přepnutí minimálně 3 pracovní dny předem. Aktivaci proxy může objednatel provést až po potvrzení dodavatele, že je konfigurace infrastruktury na přepnutí připravena.
1.2.16.4. Řešení počítá s tím, že původní IP adresa uživatele bude v případě HTTP(S) protokolu v objednatelem specifikované HTTP hlavičce v obvyklém formátu. Tuto IP adresu řešení dále propaguje až k aplikačnímu serveru tak, aby byla aplikacím objednatele k dispozici a současně ji ukládá do všech logů, které ukládají IP adresu klienta.

1.3. Operační systém serverů

1.3.1. Je použit operační systém kompatibilní se systémy typu Linux, BSD atp.
1.3.2. Provozovaný OS je vždy ve verzi s podporou aktuálních bezpečnostních aktualizací.

1.4. Firewall a zabezpečení

1.4.1. DDoS ochrana
1.4.1.1. Ochrana proti DDoS útoku je nepřetržitá, v reálném čase. Funguje automaticky s možností ručních zásahů. Použité technologie jsou přímo určeny k ochraně proti DDoS na IPv4 a IPv6.

1.4.1.2. Ochrana je určena primárně na volumetrické útoky, TCP State-Exhaustion útoky a útoky na aplikační vrstvě. Ochrana funguje proti více současným útokům v jeden okamžik.
1.4.1.3. Ochrana na ISO/OSI vrstvě 3 a 4 (ochrana sítě) je implementována minimálně na úrovni celého datacentra nebo (lépe) u poskytovatelů připojení datacentra.
1.4.1.4. Ochrana na ISO/OSI vrstvě 7 (ochrana serveru) chrání minimálně protokol HTTP.
1.4.1.5. Ochrana eliminuje útoky až do 2 Gbps příchozího (ingress) provozu s možností rozšířit kapacitu minimálně na 5 Gbps ingress provozu po jednotkách Gbps. Při výpočtech se uvažuje celkový provoz (tedy legitimní i škodlivý dohromady).
1.4.1.6. Ochrana umožňuje výrazné omezení nebo úplného odříznutí mezinárodního provozu (požadavků přicházejících mimo ČR)
1.4.1.7. Možnost úprav a nastavení vlastních pravidel a limitů pro detekci a prevenci útoků na základě žádosti objednatele včetně explicitního whitelistingu/blacklistingu.
1.4.1.8. V případě detekovaného útoku je objednatel o této skutečnosti neprodleně notifikován včetně podrobností o útoku a přijatých opatřeních. Během probíhajícího útoku je pak pravidelně informován o aktuálním stavu.
1.4.1.9. Součástí měsíčních reportů jsou detailní informace o zachycených útocích.
1.4.1.10. Součástí služby je podrobná dokumentace jak ochrana funguje, jakým způsobem útoky řeší a jaké jsou výhody/nevýhody jednotlivých opatření. Jaké jsou možnosti nastavení ochrany nad rámec výše uvedených minimálních požadavků.

1.4.2. Ochrana IPS/IDS pro detekci a prevenci dalších typů útoků
1.4.2.1. databáze pravidel se automaticky aktualizuje
1.4.2.2. systém vidí do kompletního síťového provozu
1.4.2.3. jednotlivá pravidla lze dynamicky vypínat / zapínat
1.4.2.4. pro jednotlivé pravidla lze nastavit zda se mají aplikovat v režimu IDS (pouhá detekce) nebo IPS (blokování)
1.4.2.5. poskytovatel nacení řešení pro minimálně 5 Gbps ingress provozu
1.4.2.6. objednatel zváží nasazení IPS/ IDS dle evaluace přínosů vs. nákladů (viz vyhrazená změna závazku), tj. nacenění výše se nezapočítává do nabídkové ceny

1.4.3. L4 Firewall
1.4.3.1. Možnost blokace definovaných cílových portů (TCP i UDP)
1.4.3.2. Možnost blokace ICMP
1.4.3.3. Možnost blokace na základě sítě či IP adresy zdroje či cíle

1.4.4. Webový Aplikační firewall
1.4.4.1. Automaticky aktualizovaná pravidla, minimálně OWASP core a pravidla specifická pro Drupal.
1.4.4.2. Možnost vlastních pravidel a deaktivace / konfigurace všech pravidel

1.4.4.3. Detekce robotů (legitimních i nelegitimních)
1.4.4.4. Různé možnosti reakce, minimálně:
- Blokace
- Omezení rychlosti (rate-limiting)
- Logování
1.4.4.5. poskytovatel nacení řešení jako cenu za milion prozkoumaných HTTP(S) požadavků
1.4.4.6. objednatel zváží nasazení WAF dle evaluace přínosů vs. nákladů (viz vyhrazená změna závazku), tj. nacenění výše se nezapočítává do nabídkové ceny

1.4.5. Všechny způsoby ochrany jsou v maximální možné míře transparentní z hlediska provozu a logování atp. pro další prvky, které chrání. V případě, že libovolná ochrana pro svoje fungování musí měnit IP adresu původního (legitimního) klienta, je zajištěno její předání dalším systémům obdobně jako v případě Reverzní Proxy Cache (1.6.5)

1.5. Load balancer / TLS terminátor

1.5.1. TLS
1.5.1.1. Podpora protokolu HTTP/2
1.5.1.2. Hlavní Produkční certifikáty a klíče dodá Objednatel
1.5.1.3. V ceně Řešení zajistí dodavatel vydávání a automatickou obnovu Let's Encrypt certifikátů pro všechny doprovodné a testovací domény.
1.5.1.4. Jsou použity moderní šifry tak, aby bylo možné dosáhnout SSL Labs skóre A+.

1.5.2. Výkon alespoň 2000 současně aktivních spojení / sessions

1.6. Reverzní Proxy Cache

1.6.1. Vysoce konfigurovatelná Proxy Cache. Konfigurovatelné funkce zahrnují:
1.6.1.1. Normalizace GET parametrů (např. seřazení podle abecedy).
1.6.1.2. Odstraňování zadaných parametrů (utm_source, …).
1.6.1.3. Nastavování HTTP hlaviček v requestu i v response podle různých stavů a vstupních proměnných (např. IP, User-Agent klienta, stav cache, backend server).
1.6.1.4. Volba konkrétního aplikačního server na základě dat v HTTP požadavku (typicky IP adresa nebo User-Agent).
1.6.1.5. Odstraňování a změna HTTP hlaviček.
1.6.1.6. Selektivní odstraňování Cookies.
1.6.1.7. Přesměrování na základě HTTP požadavku.
1.6.1.8. Klíč cache je možné vytvořit podle libovolného údaje z HTTP požadavku.
1.6.1.9. Konfigurovatelná doba, po kterou je vracen "zastaralý" obsah z cache, pokud origin server neodpovídá nebo má pomalou odezvu.
1.6.1.10. V případě přetížení aplikačních serverů umožnit měnit režim provozu (viz kapitola 4).

1.6.2. Vlastní konfiguraci a odpovědnost za její funkčnost je na straně Dodavatele. Objednatel zadává změnové požadavky pomocí podpory. Požadavky na změnu konfigurace jsou považovány za Běžný incident.
1.6.3. Objednatel má vždy v k dispozici aktuální konfiguraci Proxy Cache ve strojově i lidsky zpracovatelné/čitelné podobě.
1.6.4. Cachování v RAM serveru kapacita 64 GiB
1.6.5. Zasílání reálné IP adresy návštěvníka origin serveru (HTTP hlavičkou nebo PROXY protokolem)
1.6.6. Možnost invalidace celé cache nebo části (podle URL požadavku nebo HTTP hlaviček odpovědi)
1.6.7. Logování HTTP požadavků na úrovní Proxy Cache viz logování

1.7. Aplikační server

1.7.1. Fyzické nebo virtuální servery s rychlou možností rozšířit kapacitu RAM a počet jader procesoru.
1.7.2. Rozšíření kapacity nebo počtu aplikačních serverů provádí Dodavatel nejpozději do 1 pracovního dne od doručení Objednávky nebo doručení dílčí smlouvy.
1.7.3. Minimální počet aplikačních serverů je 4, každý obsahuje alespoň 4 jádra o taktu min. 3 GHz na 64 bitové architektuře Intel kompatibilní.
1.7.4. Každý aplikační server obsahuje alespoň 32 GiB RAM.
1.7.5. Výpočetní prostředky serveru (CPU, RAM) jsou vyhrazené pouze pro objednatele.
1.7.6. Každý aplikační server je schopen obsloužit alespoň 10 požadavků za sekundu na obvyklou Drupal stránku.
    1.7.6.1. Jako *obvyklá stránka* bude brána výchozí přihlašovací stránka /user
1.7.7. PHP
    1.7.7.1. Verze 7.4
    1.7.7.2. Potřebná rozšíření (extensions) PHP jsou uvedeny v příloze *Současný technický stav.*
    1.7.7.3. Řešení musí umožnit budoucí přechod na novější verze PHP bez dalších nákladů.
1.7.8. Pravidelně aktualizovaný webserver ve stabilní verzi, která není starší než 6 měsíců (pokud existuje novější), Web server musí být nginx, nebo Apache.
1.7.9. Webserver je nastaven tak, že aplikace (typicky PHP) dostává původní IP adresu klienta (v PHP typicky v $_SERVER['REMOTE_ADDR']) tak, jako by před aplikačním serverem nebyly použité žádné proxy servery nebo další prvky pracující na L7.

1.8. Databázový server

1.8.1. Fyzické nebo virtuální servery s rychlou možností rozšířit kapacitu RAM a počet jader procesoru.
1.8.2. Rozšíření kapacity nebo počtu databázových serverů provádí Dodavatel nejpozději do 3 pracovních dnů od doručení Objednávky nebo doručení dílčí smlouvy.
1.8.3. Kompatibilní s MySQL 5.7 (např. Percona 5.6, MariaDB 10.3 ...)

1.8.4. Řešení musí umožnit budoucí přechod na novější verze SQL serveru, podle aktuálních potřeb aplikace.
1.8.5. Řešení umožňuje horizontální i vertikální škálování.
1.8.6. Řešení bude provozováno v režimu s vysokou dostupností.
1.8.7. Minimální počet databázových serverů je 3, každý obsahuje alespoň 4 jádra o taktu 3 GHz na 64 bitové architektuře Intel kompatibilní.
1.8.8. Každý databázový server obsahuje alespoň 32 GiB RAM.
1.8.9. Výpočetní prostředky serveru (CPU, RAM) jsou vyhrazené pouze pro objednatele.
1.8.10. Architektura je přizpůsobena tomu, že pro většinu přístupů stačí pouze replika pro čtení - dotazy SELECT tvoří průměrně 97 % dotazů. Ve větší míře data vkládají/aktualizují jen přihlášení uživatelé (rozlišitelní dle cookie), mimo to se do db vkládají pouze řádově desítky až stovky odeslaných kontaktních/soutěžních formulářů za den.
1.8.11. Objednatel bude mít přístup k databázovému serveru pomocí dvou uživatelských účtů:
1.8.11.1. Uživatel, který má právo čtení/zápisu/modifikace všech tabulek, přidávání/editace indexů, tabulek a views
1.8.11.2. Uživatel s plným přístupem ke čtení všech dat a právem zápisu do dohodnuté množiny databázových tabulek (specifikace během realizace)
1.8.12. Pro přístup k databázovým serverům bude k dispozici nástroj Adminer (vždy v aktuální verzi), přístupný pouze pomocí protokolu HTTPS
1.8.13. K dispozici je “slow query log” (viz dále logování), na žádost je možné měnit konfiguraci long_query_time
1.8.14. Všechna data jsou uložena na discích s parametry
1.8.14.1. zápis > 30 000 iops, čtení > 50 000 iops
1.8.14.2. zápis > 300 MiB/s, čtení > 400 MiB/s
1.8.15. Objednatel má k dispozici dostupný prostor o kapacitě 60 GiB pro uložení databázových dat a jejich indexů. Ostatní data (operační systém, veškerý SW potřebný pro provoz databázového serveru, dočasné soubory, logy, binární/replikační logy atp.) se do tohoto prostoru nezapočítávají a tvoří režijní náklady dodavatele.
1.8.16. Rozšíření kapacity je objednáváno jako navýšení dostupného prostoru a cena je vypočítána jako počet GiB x aktuální počet databázových serverů v clusteru.
1.8.17. Přidání dalšího databázového serveru do clusteru je za jednotkovou cenu databázového serveru + poptávaná velikost RAM a počet CPU + aktuální kapacita úložiště v databázovém clusteru.

1.9. Diskové úložiště pro statický obsah

1.9.1. Společné úložiště přístupné ze všech aplikačních serverů.
1.9.2. Připojení k aplikačním serverům alespoň 10 Gbps.
1.9.3. Dvě úrovně rychlosti úložiště
1.9.3.1. Pomalé pro velké statické soubory (typicky audio, video)

1.9.3.1.1. Výchozí kapacita 8 TiB, možnost okamžitého rozšíření kapacity
1.9.3.1.2. zápis > 200 iops, čtení > 250 iops
1.9.3.1.3. zápis > 100 MiB/s, čtení > 150 MiB/s
1.9.3.2. Rychlé pro obrázky a další statický obsah, možnost okamžitého rozšíření kapacity
1.9.3.2.1. Výchozí kapacita 3 072 GiB
1.9.3.2.2. zápis > 10 000 iops, čtení > 15 000 iops
1.9.3.2.3. zápis > 250 MiB/s, čtení > 250 MiB/s
1.9.4. Diskové úložiště podporuje tzv. snapshoty.
1.9.5. Diskové úložiště je provozováno s redundancí na úrovni alespoň RAID6 nebo lepší.

1.10. Paměťové úložiště (cache server)

1.10.1. Kompatibilní jako cache pro Drupal, tj. Memcache nebo Redis.
1.10.2. mohou být součástí aplikačních serverů nebo samostatně
1.10.3. Kapacita min 16 GiB, rozděleno do alespoň 2 instancí.
1.10.4. Aktuální zatížení viz příloha *Současný technický stav.*

1.11. Server pro vyhledávání

1.11.1. Jeden server Apache Solr, pro účely vyhledávání obsahu v rámci administrace. V budoucnu na vyžádání objednatele musí být dodavatel schopen nahradit Solr server serverem Elaticsearch.
1.11.2. Minimální kapacita 20 GiB.
1.11.3. Aktuální zatížení a kapacita viz příloha *Současný technický stav.*
1.11.4. Konfiguraci a správu vyhledávacího serveru provádí Dodavatel.

1.12. Logování

1.12.1. Všechny HTTP požadavky na infrastrukturu jsou logovány a agregovány na úroveň jednotlivého HTTP požadavku s ukládáním informací minimálně v rozsahu NCSA combined.
1.12.2. U požadavků z origin serverů je logována doba zpracování požadavků na origin serveru.
1.12.3. Dočasně a na vyžádání (pro účely ladění) je možné do logu ukládat HTTP hlavičky z odpovědi origin serveru.
1.12.4. K dispozici jsou na jednom místě agregované PHP error logy ze všech origin serverů, s logováním na úrovni Notice.
1.12.5. K dispozici je MySQL slow query log
1.12.6. Na vyžádání je možné zapnout zaznamenávání MySQL query logu po dobu až 24 hodin.
1.12.7. K dispozici je Drupal log, s parametry jako PHP error log. Drupal log není ukládán do MySQL databáze Drupalu.
1.12.8. Error log PHP a log Drupalu je k dispozici v reálném čase, všechny ostatní logy jsou k dispozici se zpožděním maximálně 5 minut.
1.12.9. Všechny logy jsou agregovány do jednoho systému, který je umožňuje prohledávat a zobrazovat trendy (např. ELK stack). (není potřeba k datu spuštění, viz sekce Milníky)
1.12.10. Všechny logy jsou rotovány po dnech a logicky pojmenovány tak, aby je bylo možné automaticky zpracovávat.
1.12.11. Logy jsou uchovávány za posledních 12 měsíců.

1.12.12. Úložiště logů není dodatečně zpoplatněno nad základní cenu Řešení.

1.13. Zálohování

1.13.1. Veškerá data z Diskového úložiště se zálohují minimálně s denní frekvencí a je uchováno minimálně 30 posledních denních, 12 posledních týdenních a 12 posledních měsíčních

1.13.2. Záloha databáze se provádí každé dvě hodiny a je uchováno posledních 30 dní záloh. Jedna denní záloha je konzistentní s příslušnou zálohou souborových dat.

1.13.3. Prováděné zálohování neovlivňuje výkon ani funkce Řešení.

1.13.4. Objednatel má zajištěn přímý přístup k zálohám. Formát, způsob a orientační časová náročnost obnovy záloh je dokumentována.

1.13.5. Objednatelem vymezený rozsah záloh je v dohodnutých intervalech synchronizován na prostředky Objednatele pomocí dohodnutého a šifrovaného protokolu sítě internet.

1.14. Monitoring a alerting

1.14.1. Následující metriky má Objednatel online přístupné v podobě denních, týdenních, měsíčních a ročních grafů:

1.14.1.1. Vytížení internetové konektivity

1.14.1.2. Počet všech HTTP požadavků za sekundu, rozlišené podle požadavků, které byly/nebyly obsloužené z cache.

1.14.1.3. Počet HTTP požadavků na stránky (tedy mimo assety) za sekundu, rozlišené podle požadavků, které byly/nebyly obsloužené z cache.

1.14.1.4. Zátěž load balanceru

1.14.1.5. Zátěž proxy cache

1.14.1.6. Zaplnění proxy cache

1.14.1.7. Počet požadavků na aplikační servery za sekundu.

1.14.1.8. Zátěž aplikačních serverů

1.14.1.9. Počet databázových dotazů za sekundu s rozlišením podle druhu

1.14.1.10. Zátěž databázových serverů

1.14.1.11. Počet požadavků na paměťové úložiště za sekundu s rozlišením hit/miss.

1.14.1.12. Zaplnění paměťového úložiště

1.14.1.13. Vytížení LAN

1.14.1.14. Vytížení diskového úložiště

1.14.1.15. Zaplnění diskového úložiště

1.14.2. Všechny obvyklé metriky navíc k bodu 1.14.1 (zejména ukazatele load balanceru, proxy cache, aplikačního serveru, paměťového úložiště, databázového serveru) je možné ukládat do vhodné time series databáze (např. Prometheus, InfluxDB popř. Graphite atp.) a je možné je s minimální prodlevou (zpoždění do 1 minuty) zobrazovat v uživatelsky konfigurovatelných (časové omezení, skládání více metrik) grafech a dashboardech (např. Grafana). Možnost zapojení externích dat do tohoto systému (např. MySQL databáze).

1.14.2.1. Příklad sledovaných metrik, nejedná se o kompletní výčet:

1.14.2.1.1. Load balancer (počet požadavků, load)

1.14.2.1.2. Reverzení proxy cache (počet požadavků, hits, misses, zaplnění cache, počet objektů)
1.14.2.1.3. Aplikační server - pro každou instanci (počet požadavků, požadavky podle stavového kódu odpovědi, běhové chyby, load jednotlivých serverů)
1.14.2.1.4. Databázovy servery (load, počet dotazů za vteřinu a jejich typy)
1.14.2.1.5. Paměťové úložiště - pro každou instanci (počet požadavků hits, misses, zaplnění cache, počet objektů)
1.14.2.2. Příklad otázek, na které Objednatel chce znát odpověď:
1.14.2.2.1. Graf poměru návštěvnosti z vyhledávačů pro doménu XY za období AB.
1.14.2.2.2. Průměrná doba renderování necachované URL za den
1.14.2.3. Příklad filtrů (a jejich kombinací), které chceme používat
1.14.2.3.1. Časové období OD-DO
1.14.2.3.2. Domény (1 - všechny)
1.14.2.3.3. Požadavek ne/obsloužen z proxy cache
1.14.2.3.4. Ne/přihlášený uživatel (podle cookie)
1.14.2.3.5. Crawler/normální návštěvník (podle UA)
1.14.2.3.6. Filtrování v názvu URL
1.14.3. Stav a zátěž a využití kapacity infrastruktury, a odezva určených URL je automaticky monitorována vhodným systémem (např. Icinga 2).
1.14.3.1. Pro monitorované hodnoty (SLI) jsou dohodou určeny příslušné hranice (SLO) při jejichž překročení je Objednatel dohodnutým způsobem (mail, Slack, Pagerduty…) notifikován.

2. Technické požadavky na testovací infrastrukturu

2.1. Použitá nastavení a verze všech komponent jsou vždy totožné jako u produkční infrastruktury.
2.2. Testovací infrastruktura se od produkční liší pouze výkonem, kapacitou, způsobem zálohování, logování a požadovanou dostupností.
2.3. Synchronizace dat z produkční infrastruktury na testovací.
2.3.1. Minimálně 1x týdně probíhá automatický import databáze
2.3.2. Přenos databáze je možné jednoduše spustit manuálně (očekávaná doba běhu takového importu může být 1-2h).
2.3.3. Minimálně 1x za 2 týdny probíhá synchronizace statického obsahu
2.3.4. Možnost jednoduše spustit synchronizaci nejnovějšího statického obsahu.
2.4. Log soubory se uchovávají 14 dní.
2.5. Data z testovací infrastruktury nejsou zálohována.
2.6. Testovací infrastruktura nemusí podporovat sběr metrik a chyb za běhu.
2.7. Testovací infrastruktura je monitorována jen na základní funkčnost.

3. Požadavky na publikování aplikací (deploy)

3.1. Možnost provádění publikaci skrze robustní workflow - prostřednictvím jedné akce / příkazu (s potvrzením) je možné provést deploy kódu na všechny aplikační servery.
3.2. Deploy na aplikační servery musí být možný i pomocí Deployer z prostředí Bitbucket pipeline (nebude potřeba k datu spuštění)

3.2.1. Jde tedy o zpřístupnění webserverů via SSH z IP adres Bitbucketu

3.3. SSH přístup na příkazovou řádku jako neprivilegovaný uživatel, ale s právem měnit, číst a spouštět stejné soubory jako webserver/php.

3.4. Je možné spouštět drush příkazy.

3.5. K dispozici je SFTP protokol, rsync, curl, git client a řádkový klient mysql.

3.6. Je možné spravovat adresář sites/default/files, tj. vytvářet, editovat a mazat v něm adresáře a soubory.

4. Požadavky na provoz

4.1. Na žádost a ve spolupráci s Dodavatelem je možné zadávat a modifikovat pravidelně spouštěné úlohy (např. cron)

4.2. Úlohy je možné spouštět každou minutu, jsou podporovány všechny příkazy dostupné na aplikačním serveru, zejména drush.

4.3. Produkční i testovací Infrastruktura umožňuje tři režimy provozu:

4.3.1. Běžný provoz.

4.3.2. Přetížení - dočasné nepoužívání aplikačních serverů pro specifikované weby a poskytování pouze stránek z proxy cache. U nenacachované stránky se zobrazuje customizovatelná statická informace.

4.3.3. Kritický režim - náhrada celého jednotlivého (či všech) webu customizovatelnou statickou HTML stránkou o výjimečné události optimalizovanou na vysokou nárazovou návštěvnost (alespoň 100 000 requestů za minutu);

4.4. Infrastruktura umožňuje ruční přepnutí režimu a customizaci statické HTML stránky/informace a jejích assetů (CSS, obrázky, JS) použité v těchto režimech.

4.5. Infrastruktura umožňuje automatické přepnutí režimu provozu jednotlivého webu na základě dosažených metrik (např. zátěž, počet Návštěvníků webových stránek, apod.) dohodnutých s Objednatelem.

5. Dokumentace

5.1. Veškerá níže zmíněná dokumentace je v češtině nebo angličtině.

5.2. Správnost a úplnost dokumentace je kontrolována a aktualizována každé 3 měsíce.

5.3. Je k dispozici podrobný popis a diagramy produkční a testovací infrastruktury včetně všech použitých komponent a jejich konfigurace.

5.4. Kompletní uživatelská i správcovská dokumentace všech komponent, které nejsou Open Source.

5.5. Dokumentace měřených metrik, způsobu měření a vyhodnocování

5.6. Dokumentace k zabezpečení a procesům (např. VPN, ukládání hesel, TLS atd.) zejména pro účely auditů a kontrol třetích stran.

6. Organizační požadavky

6.1. Jednou za 2 až 3 měsíce se potkávat na společné schůzce (osobně nebo online) svolané Objednatelem, kde bude možné řešit směry dalších úprav/optimalizací infrastruktury.

6.2. měsíční vykazování hodin týkajících se servisní podpory a plnění požadavků Objednatele

7. Licence

7.1. Všechny komponenty Infrastruktury jsou provozovány bez licenčních poplatků ze strany Objednatele.

7.2. Objednatel prefereruje použití open-source software, na jeho použití trvá u komponent:

- 7.2.1. Aplikační server (webserver)
- 7.2.2. Databázový server
- 7.2.3. Paměťové úložiště (cache server)
- 7.2.4. Server pro vyhledávání

8. Podpora a údržba

8.1. Dodavatel 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.

8.2. Objednatel má k dispozici telefonní hotline v režimu 24 hodin / 7 dnů v týdnu.

8.3. Servisní doba Dodavatele je 365 dní v roce, 7 dní v týdnu, 24 hodin denně.

8.4. Je písemně dohodnuto jedno Servisní okno v maximálním rozsahu 2 hodiny měsíčně, v pravidelném intervalu (např. 2. neděle v měsíci 02:00-04:00) v době, kdy nejméně omezuje potřeby Objednatele.

8.5. Minimální dostupnost infrastruktury je 99.95 % v každém kalendářním měsíci.

8.6. Nedostupnost je zjištěna monitorovacím nástrojem třetí strany, který neprovozuje Dodavatel a na kterém se Objednatel s Dodavatelem dohodnou včetně metodiky měření. Nedostupnost též může být nahlášena při jejím zjištění Objednatelem. Vždy bude zjišťována minimálně:

- 8.6.1. Funkčnost a výkon Firewallu
- 8.6.2. Funkčnost a výkon Load Balanceru
- 8.6.3. Funkčnost a výkon Reverzní Proxy Cache
- 8.6.4. Funkčnost všech aplikačních serverů (případné přetížení vinou Objednatele nelze považovat za nedostupnost služby)
- 8.6.5. Funkčnost všech databázových serverů (případné přetížení vinou Objednatele nelze považovat za nedostupnost služby)
- 8.6.6. Funkčnost diskového a paměťového úložiště
- 8.6.7. Funkčnost serveru pro vyhledávání

8.7. 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.

8.8. 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	postihuje více než 20 % návštěvníků, web pro ně není funkční	1 hodina	4 hodiny
2 - Vážný incident	HTTP požadavky na weby jsou z 80 % splněny pro nepřihlášené návštěvníky, web není funkční pro administrátory a redakci	4 hodiny	24 hodin
3 - Běžný incident	závada umožňující práci systému pro všechny uživatele s pomocí náhradního pracovního postupu	1 pracovní den	3 pracovní dny
4 - Běžný požadavek	např. úprava konfigurace nebo drobná chyba, která neovlivňuje činnost	2 pracovní dny	5 pracovních dnů

8.9. Do 5. dne každého měsíce je Objednateli zaslán report, který obsahuje:
- 8.9.1. Dostupnost služby
- 8.9.2. Přehled využití servisního okna
- 8.9.3. Přehled řešených Incidentů s výsledným stavem
- 8.9.4. Přehled řešených bezpečnostních incidentů včetně detailní analýzy (minimálně objem útoku, délka trvání, typ útoku, cíle útoku, způsob obrany, důsledky útoku).
- 8.9.5. Rychlostní / výkonnostní trendy infrastruktury
- 8.9.6. Využití kapacity
- 8.9.7. Doporučení k opatřením
- 8.9.8. Výkaz hodin servisních prací

8.10. Na základě žádosti, zaslané v dostatečném předstihu (v režimu 8 hodin / 5 dnů v týdnu) vyhradí Dodavatel Objednateli pracovníka na Objednatelem určený den a daný počet servisních hodin (v režimu 24 hodin / 7 dnů v týdnu):
- 8.10.1. při oznámení alespoň 2 kalendářní dny dopředu vyhradí Dodavatel až 2 servisní hodiny.
- 8.10.2. při oznámení alespoň 5 kalendářních dní dopředu vyhradí Dodavatel až 4 servisní hodiny.
- 8.10.3. při oznámení alespoň 8 kalendářních dnů dopředu vyhradí Dodavatel až 6 servisních hodin.

8.11. 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 Dodavatele či autora této součásti. V případě chyb s CVSS score 8 a vyšším je lhůta 7 kalendářních dnů.

8.12. Je veden záznam o servisních zásazích na Infrastruktuře s přesnými záznamy času, pracovníků podílejících se na zásahu a popis provedené operace.
8.13. Neexistují společné přístupové účty, každý pracovník Dodavatele má samostatný přístup vedený na jeho jméno.
8.14. Součástí ceny Podpory a Údržby je **měsíčních 10 hodin** určených na správu a rekonfiguraci Infrastruktury.
8.15. V případě ukončení poskytování služby předá poskytovatel objednateli aktuální data z databází a veškeré další soubory použité pro provozování služby (zvuky, obrázky videa atp.) a poskytne součinnost při migraci na jinou infrastrukturu.
8.16. Součinností při migraci na jinou infrastrukturu je myšleno poskytnutí odborného školení zaměstnancům Objednatele, na další rozvoj a provoz v rozsahu 3 (tří) pracovních dnů v budově Objednatele. Cena tohoto školení byla Dodavatelem zahrnuta v ceně úvodní migrace (viz. Příloha – Cenová nabídka poskytovatele). Na školení Dodavatel Objednateli zejména:
    8.16.1. 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;
    8.16.2. popíše architekturu celé infrastruktury a jejích prvků, vysvětlí vazby mezi jednotlivými částmi;
    8.16.3. pomůže navázat na jakoukoliv nedokončenou práci, požadavek, rozvoj či incident, včetně toho, že bude pokračovat v práci zatímco ji pracovníci Objednatele budou sledovat, aby pochopili, jak mají dále sami pokračovat;
    8.16.4. 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;

9. Milníky

Do 7 dnů od účinnosti první dílčí smlouvy

Infrastruktura připravena pro migraci dat a testování

Do 30 dnů od účinnosti první dílčí smlouvy

Spuštění ostrého provozu

Do tří měsíců od spuštění

Monitorovací dashboard - 1.12.9

Přílohy

Současný technický stav

Aktuálně probíhá zveřejnění na produkci 2-5x týdně bez součinnosti poskytovatele infrastruktury.

Pro verzování kódu je použit komerční bitbucket.org.

- Drupal 7 (irozhlas.cz, rozhlas.cz)
    - Jedna instance drupalu s jednou databází
    - 1.26mil nodů (v tabulce “node” - stav k 28. 1.2022)
    - 1.7mil souborů (v tabulce “file_managed”)
- Loadbalancer - Nginx
    - Avg 400req/s, během dne 550req/sec
    - Datový tok ani ne 100Mb/sec
    - Průměrná velikost jedné response
    - irozhlas.cz - 32kB
    - *.rozhlas.cz - 360kB (průměr ovlivněn stahováním MP3 souborů)
- Proxy cache - proprietární řešení postavené nad drupal modulem Boost
    - Nemáme více informací
- Webservery - Apache
    - Přibližně 14req/s
    - PHP 7.3.27
        - Extensions: mysqlnd, opcache, pdo, xml, bcmath, bz2, calendar, ctype, curl, dom, exif, fileinfo, ftp, gd, gettext, iconv, igbinary, imagick, json, mbstring, msgpack, mysqli, pdo_mysql, phar, posix, readline, shmop, simplexml, soap, sockets, sysvmsg, sysvsem, sysvshm, tokenizer, wddx, xmlreader, xmlwriter, xsl, yaml, zip, memcached
        - Důležitá nastavení:
            - Allow_url_fopen: on
            - Max_execution_time: 240
            - Max_input_time: 360
            - Max_input_vars: 20000
            - Memory_limit: 1024M
            - Post_max_size: 896M
            - Upload_max_filesize: 1G
            - Short_open_tag: on
        -
    - 4 webservery (každý čtyřjádrový 3Ghz)
- Drupal cache - Memcache
    - Tři servery mají 4GB memcache instanci
    - Jeden server má 2x 2GB memcache instance
- Databáze - MariaDB (10.3.31) v Galera clusteru (3 nodes)
    - Velikost DB (včetně indexů) 40G
    - 96 % dotazů jsou SELECT
    - Průměrně 1800 dotazů za vteřinu, ve špičce kolem 2200

- SOLR
    - Jeden server
    - Uloženo zhruba 3m entit, 11GB na disku
    - Během pracovní doby řádově vyšší desítky požadavků za minutu, v noci téměř bez provozu
- Množství dat
    - Zhruba 9TB, z toho 6.8TB jsou audiosoubory na “pomalejším disku”

Odhad nárůstu zátěže infrastruktury

- Měsíční nárůst obsahu
    - 6500 drupalových uzlů
    - 4300 audio souborů
        - Za poslední měsíc 80GB
    - 8000 obrázků
        - Za poslední měsíc 10GB
- Traffic
    - Nárůst 15 % každých 12 měsíců (predikce na základě návštěvnosti 2019-2022)

Současný provoz na loadbalanceru