Příloha č. 6 – Technická specifikace

[1. Předmět veřejné zakázky 3](#_Toc206404014)

[2. Rozdělení zakázky a základní specifikace 5](#_Toc206404015)

[2.1. Část A: Kubernetes infrastruktura a GitOps 5](#_Toc206404016)

[2.2. Část B: Aplikační cloud pro Drupal 5](#_Toc206404017)

[2.3. Část C: Cloudová platforma mujRozhlas a další digitální produkty 5](#_Toc206404018)

[3. Část A: Kubernetes infrastruktura a GitOps 6](#_Toc206404019)

[3.1. Požadavky na cloudovou infrastrukturu 6](#_Toc206404020)

[3.2. Požadavky na migraci aplikací 6](#_Toc206404021)

[3.3. Síťová infrastruktura a bezpečnostní opatření 6](#_Toc206404022)

[3.4. Monitoring a observabilita 7](#_Toc206404023)

[3.5. Zálohování a Disaster Recovery 7](#_Toc206404024)

[3.6. Aktuální využití zdrojů 7](#_Toc206404025)

[4. Část B: Aplikační cloud pro Drupal 7](#_Toc206404026)

[4.1. Současný technický stav 8](#_Toc206404027)

[4.2. Požadavky na cloudovou infrastrukturu 9](#_Toc206404028)

[4.2.1. Požadavky na výkon 9](#_Toc206404029)

[4.2.2. Požadavky na datacentrum a zapojení serverů 9](#_Toc206404030)

[4.2.3. Operační systém serverů 10](#_Toc206404031)

[4.2.4. Load balancer / TLS terminátor 10](#_Toc206404032)

[4.2.5. Reverzní Proxy Cache 11](#_Toc206404033)

[4.2.6. Aplikační server 11](#_Toc206404034)

[4.2.7. Databázový server 12](#_Toc206404035)

[4.2.8. Diskové úložiště pro statický obsah 13](#_Toc206404036)

[4.2.9. Paměťové úložiště (cache server) 14](#_Toc206404037)

[4.2.10. Server pro vyhledávání 14](#_Toc206404038)

[5. Část C: Cloudová platforma mujRozhlas a další digitální produkty 14](#_Toc206404039)

[5.1. Současný technický stav 14](#_Toc206404040)

[5.2. Technické parametry virtualizované HW infrastruktury 15](#_Toc206404041)

[5.3. Úložiště 16](#_Toc206404042)

[5.4. Zálohování 16](#_Toc206404043)

[5.5. Konektivita 16](#_Toc206404044)

[5.6. Administrační rozhraní virtualizace 16](#_Toc206404045)

[5.7. API virtualizace 17](#_Toc206404046)

[5.8. Výkonnostní požadavky 17](#_Toc206404047)

[6. Obecné požadavky na datové centrum 17](#_Toc206404048)

[6.1. Redundance, architektura, propojení cloudů, lokality 17](#_Toc206404049)

[6.4. Požadavky na provoz 18](#_Toc206404050)

[6.5. Technické požadavky na produkční infrastrukturu 18](#_Toc206404051)

[6.6. Technické požadavky na testovací infrastrukturu 20](#_Toc206404052)

[6.7. Požadavky na publikování aplikací (deploy) 20](#_Toc206404053)

[6.8. Monitoring a alerting 21](#_Toc206404054)

[6.9. Zálohování 22](#_Toc206404055)

[6.10. Logování 23](#_Toc206404056)

[6.11. Provozní požadavky na datacentra a zapojení serverů 23](#_Toc206404057)

[6.12. Bezpečnostní požadavky 24](#_Toc206404058)

[6.12.1. DDoS ochrana 24](#_Toc206404059)

[6.12.2. Ochrana IPS/IDS pro detekci a prevenci dalších typů útoků 25](#_Toc206404060)

[6.12.3. L4 Firewall 25](#_Toc206404061)

[6.12.4. Webový Aplikační firewall (WAF) 26](#_Toc206404062)

[6.13. Dokumentace 26](#_Toc206404063)

[6.14. Licence 26](#_Toc206404064)

[6.15. Podpora a údržba 26](#_Toc206404065)

[6.16. Organizační požadavky 27](#_Toc206404066)

[6.17. Milníky 27](#_Toc206404067)

[6.18. Migrace 27](#_Toc206404068)

[**PŘÍLOHA č. 1 – POŽADAVKY NA MIGRACI** 28](#_Toc206404069)

[**1. Úvod a účel** 28](#_Toc206404070)

[Přílohy 30](#_Toc206404071)

# Předmět veřejné zakázky

Předmětem veřejné zakázky je zajištění provozu cloudových služeb pro jednotlivé digitální/online projekty a produkty divize Marketing a digitální služby Českého rozhlasu dle aktuálních potřeb, zajištění jejich modernizace a rozvoje, zavedení metodologie GitOps a zajištění případné migrace dat.

**Cílem projektu je:**

* zvýšení bezpečnosti serverové a datové infrastruktury
* zajištění vysoké dostupnosti a redundance
* optimalizace provozních nákladů a efektivnější využívání zdrojů
* zlepšení možnosti monitorování a řízení provozu
* implementace moderního přístupu ke správě infrastruktury díky využití technologie Kubernetes
* unifikace prostředí za pomocí GitOps metodologie
* postupná migrace z aktuálního stavu do Kubernetes na novou infrastrukturu
* dodávka a provoz specializovaného aplikačního cloudu pro redakční systém Drupal
* provoz a rozvoj virtualizované cloudové platformy pro projekt digitální produkty a služby

**Cloudové prostředí bude sloužit zejména pro provozování následujících aplikací:**

* Kubernetes Cluster, zejména:
	+ Rancher RKE2
	+ ArgoCD
	+ Hashicorp Vault
	+ Keycloak
	+ Terraform
	+ Prometheus
	+ Thanos
	+ Alertmanager
	+ Grafana
	+ Uptime Kuma
	+ Better Stack
	+ Grafana Loki
	+ Cloudflare
	+ WireGuard
	+ S3 kompatibilní objektové úložiště
	+ PostgreSQL (managed)
* CMS Drupal 7
* CMS Drupal 10
* custom CMS Diego
* různá API
* audio platforma mujRozhlas
* zpravodajská platforma iROZHLAS
* ad-hoc webové aplikace, zejména:
	+ Ježíškova vnoučata
	+ Ostrov Olomouc
	+ Platí To
	+ a další
* další digitální/online aplikace ČRo.

Cloudová platforma (dále také jako „platforma“) je tvořena infrastrukturní / HW vrstvou a SW vrstvou. Obě tyto vrstvy budou ve správě dodavatele služeb a budou rozvíjeny na základě požadavků a potřeb zadavatele.

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.

**Zajištění provozu cloudové platformy znamená:**

1. poskytnutí virtualizované HW infrastruktury včetně monitoringu (infrastrukturní cloud)
2. správu, provoz a rozvoj HW a SW prostředí potřebného pro běh internetových aplikací a nástrojů zadavatele. Jde zejména o
	1. optimalizace HW infrastruktury a SW prostředí na požadovaný provoz aplikací
	2. správu, monitoring a rozvoj nezbytného SW, tj. OS a middleware.
	3. zajištění bezpečnosti a údržby SW prostředí (aktualizace, zálohování atd.)
3. provozování servisní podpory prostřednictvím online helpdesku a telefonní hotline
4. udržování aktuální dokumentace platformy

**Součástí provoz cloudové platformy není:**

1. správa aplikační vrstvy projektů, tj. správa samotných aplikací jako např. integrační nástroj rAPI, CMS Drupal a další
2. správa DNS serverů
3. správa SMTP serverů.

# Rozdělení zakázky a základní specifikace

## Část A: Kubernetes infrastruktura a GitOps

* Migrace workloadů z VM do kontejnerového prostředí Kubernetes pomocí Rancher RKE2.
* Vysoká dostupnost, redundance a bezpečnost díky GitOps (ArgoCD, Vault).
* IaC pomocí Terraform (včetně Cloudflare, Keycloak, infrastruktura).
* Úložiště: S3 kompatibilní objektové úložiště, podpora managed databází (např. PostgreSQL).
* Monitoring & observability: Prometheus, Thanos, Alertmanager, Grafana, Uptime Kuma.
* Centralizované logování: Grafana Loki, alerting, přístup chráněn SSO.
* Disaster recovery: měsíční zálohy, test obnovy každé 3 měsíce.
* Síťová segmentace: PROD, STAGE, DEV, DevOps; VPN: WireGuard.

## Část B: Aplikační cloud pro Drupal

* Provoz cca 60 webů na Drupal 7, oddělení částí infrastruktury pro konkrétní skupiny aplikací
* Reverzní proxy cache, oddělení přihlášených/anon. uživatelů, HTTP/2, TLS A+.
* Datacentrum TIER III+: 2 dieselgenerátory, redundantní napájení/chlazení, firewall, WAF, IDS/IPS.
* Servery: min. 4 aplikační servery, každý 4 jádra @3GHz, 32GB RAM, rozšíření do 1 dne.
* Virtualizace: 17 VM, 178 vCPU, 820 GB RAM, 20 TB úložiště
* Databáze: HA, škálovatelnost, zálohy každé 2h, uchování 30 dní.
* Úložiště: pomalé (audio), rychlé (obrázky); RAID6+, snapshoty.
* Monitoring: široké spektrum metrik a filtrů, Grafana dashboardy, alerting.
* Deploy: Bitbucket pipelines, Deployer, SSH přístup, drush, rsync, git, SFTP.
* Servis a podpora: helpdesk 24/7, měsíční reporty, školení, SLA, měsíčně 10 hodin podpory.

## Část C: Cloudová platforma mujRozhlas a další digitální produkty

* VMware vCloud Director ≥ 10.2, Veeam zálohování.
* Virtualizace: 86 VM, 439 vCPU, 845 GB RAM, 41,7 TB úložiště (3 výkonnostní úrovně).
* Síť: 10 Gbps interně, 1 Gbps veřejně, 12 IPv4, IPv6 /56 segment.
* Bezpečnost: DDoS ochrana (1–5 Gbps), WAF, L4 firewall, IDS/IPS.
* Dokumentace: aktualizace každé 3 měsíce, měsíční reporty.
* Migrace: bez výpadku, max. 4h výpadků celkově v nočních oknech.
* Školení: rozsah 3 dny, včetně přístupů, hesel a architektury platformy.
* Lokace
	+ Cloudová platforma pro mujRozhlas (část C), která je předmětem této veřejné zakázky, se nesmí nacházet v datovém centru, kde bude umístěn aplikační cloud pro Drupal (část B) viz rámcová dohoda.

# Část A: Kubernetes infrastruktura a GitOps

V případě nesplnění některého z požadavků nabídněte alternativu včetně odůvodnění. Klademe také důraz na maximální využití open source nástrojů.

## Požadavky na cloudovou infrastrukturu

* **Kubernetes** bude sloužit jako hlavní platforma pro provoz aplikací pomocí **Rancher RKE2 engine**.
* Řešení nesmí být vázáno na jednoho cloudového dodavatele (**bez vendor lock-inu**).
* Využití **Infrastructure as Code (IaC)** pro správu prostředí prostřednictvím Terraform.
* Úložiště dat bude realizováno formou **S3 kompatibilního objektového úložiště**.
* Podporovány budou **managed databázové služby** (např. PostgreSQL).

## Požadavky na migraci aplikací

* Veškeré aplikace budou provozovány výhradně v kontejnerech **Docker**.
* Správa konfigurace proběhne pomocí **ArgoCD** a **Hashicorp Vault**.
* Logování aplikací bude centralizováno v **Grafana Loki**, logy musí být ve standardizovaném formátu.
* **Žádné aplikace nebudou využívat lokální úložiště**, veškerá data budou ukládána do S3 úložiště.

## Síťová infrastruktura a bezpečnostní opatření

* **Cloudflare** bude poskytovat **DDoS ochranu, WAF, DNS a CDN**.
* Veškerá **Cloudflare** konfigurace bude probíhat pomocí **Terraform**
* Využití **WireGuard VPN** pro bezpečnou komunikaci mezi ČRO a cloudovým prostředím.
* Implementace **Single Sign-On (SSO)** pomocí **Keycloak** s možností integrace s Active Directory.
* Konfigurace **Keycloak** musí být pomocí **Terraform**
* Oddělená síťová a aplikační prostředí: **PROD, STAGE, DEV a DevOps**.

## Monitoring a observabilita

* Monitorovací systém založený na **Prometheus Stack** (Prometheus, Thanos, Alert Manager, Grafana).
* Implementace alertingu s integrací do **e-mailu či aplikací 3. stran**
* **Uptime monitoring** prostřednictvím **Uptime Kuma** a **Better Stack**.
* Grafické vizualizace v **Grafaně**, přístup chráněn **SSO**.

## Zálohování a Disaster Recovery

* Pravidelné **měsíční zálohy databází** se simulací obnovy jednou za tři měsíce.
* Uchování **posledních dvou záloh** (minimálně **2 TB úložného prostoru**).
* Failover plán umožňující přepnutí **STAGE prostředí na produkční v případě výpadku**.
* Z failover cvičení musí být záznam pro audit

## Aktuální využití zdrojů

|  |  |  |  |
| --- | --- | --- | --- |
| **VMs count** | **Total CPU count** | **Total Memory GB** | **Total Disk GB** |
| 128 | 673 | 2025 | 63100 |

**2.6 Plánované odhadované využití zdrojů po konci projektu**

|  |  |  |  |
| --- | --- | --- | --- |
| **VMs count** | **Total CPU count** | **Total Memory GB** | **Total Disk GB** |
| 51 | 409 | 1178 | 44270 |

# Část B: Aplikační cloud pro Drupal

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 dodavatele. Bližší a technické informace k aktuálnímu stavu jsou rozepsány v kapitole tohoto dokumentu *Současný technický stav.*

## Současný technický stav

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

Přesný sizing lze nalézt v příloze “EXTERNAL- CRo infra analysis and sizing.xlsx”

Pro verzování kódu je použit komerční GitHub.

* 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 audio soubory na “pomalejším disku”

## Požadavky na cloudovou infrastrukturu

### Požadavky na výkon

* Řešení obslouží zátěž současné infrastruktury bez poklesu rychlosti – viz část *Současný technický stav.*
* Řešení je rozděleno na tři hlavní části (irozhlas.cz, \*.rozhlas.cz a administrace) - přetížení vyvolané jednou z nich nesmí způsobit nedostupnost jiné části.
* Pro odbavování audií je využita separátní doména (např. audio.rozhlas.cz) s vlastním LB
* 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.

### Požadavky na datacentrum a zapojení serverů

* Dostupnost služeb datacentra alespoň 99.95 % ročně
* Garantováno minimálně 72 hodin provozu při výpadku el. energie
* Minimálně 2 dieselgenerátory
* Redundance všech komponent alespoň N+1
* Redundantní chlazení
* Protipožární systém, automatický hasící systém
* Přístup na datový sál pomocí dvou faktorů (čip / biometrika, čip / PIN, klíč / pin, …)
* Kamerový systém s uchováváním záznamů
* K infrastruktuře nemají přístup jiné osoby, než pověřené Dodavatelem
* Minimálně 2 nezávislé optické trasy konektivity
* Přímá konektivita do NIX
* Neomezený datový přenos v rámci ČR i mimo ČR.
* Konektivita minimálně 5 Gbps bez ohledu na použitou trasu.
* Použito IPv4 i IPv6.
* Servery a síťové prvky propojeny vyhrazenou LAN 10 Gbps
* Celá infrastruktura a procesy dodavatele jsou připraveny na to, že zadavatel může potřebovat předřadit celému řešení jednu popř. více proxy (ať už od dodavatele, svoje či třetí strany).
	+ Nasazení takovýchto proxy je možné zvlášť pro testovací i produkční prostředí.
	+ Dodavatel upraví konfigurace do 30 dnů po sdělení zadavatele, že má v plánu takové řešení nasadit. Zadavatel sdělí dodavateli IP adresy nebo URL kde jsou k dispozici IP adresy těchto proxy a jak často je třeba seznam aktualizovat.
	+ Před faktickou aktivací proxy (typicky změnou DNS záznamů) zadavatel informuje o přesném datu a času přepnutí minimálně 3 pracovní dny předem. Aktivaci proxy může zadavatel provést až po potvrzení dodavatele, že je konfigurace infrastruktury na přepnutí připravena.
	+ Řešení počítá s tím, že původní IP adresa uživatele bude v případě HTTP(S) protokolu v zadavatelem specifikované HTTP hlavičce v obvyklém formátu. Tuto IP adresu řešení dále propaguje až k aplikačnímu serveru tak, aby byla aplikacím zadavatele k dispozici a současně ji ukládá do všech logů, které ukládají IP adresu klienta.

### Operační systém serverů

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

### Load balancer / TLS terminátor

* TLS
	+ Podpora protokolu HTTP/2
	+ Hlavní Produkční certifikáty a klíče dodá zadavatel
	+ V ceně řešení zajistí dodavatel vydávání a automatickou obnovu Let’s Encrypt certifikátů pro všechny doprovodné a testovací domény.
	+ Jsou použity moderní šifry tak, aby bylo možné dosáhnout SSL Labs skóre A+.
* Výkon alespoň 2000 současně aktivních spojení / sessions

### Reverzní Proxy Cache

* Vysoce konfigurovatelná Proxy Cache. Konfigurovatelné funkce zahrnují:
	+ Normalizace GET parametrů (např. seřazení podle abecedy).
	+ Odstraňování zadaných parametrů (utm\_source, …).
	+ Nastavování HTTP hlaviček v requestu i v response podle různých stavů a vstupních proměnných (např. IP, User-Agent klienta, stav cache, backend server).
	+ Volba konkrétního aplikačního server na základě dat v HTTP požadavku (typicky IP adresa nebo User-Agent).
	+ Odstraňování a změna HTTP hlaviček.
	+ Selektivní odstraňování Cookies.
	+ Přesměrování na základě HTTP požadavku.
	+ Klíč cache je možné vytvořit podle libovolného údaje z HTTP požadavku.
	+ Konfigurovatelná doba, po kterou je vracen “zastaralý” obsah z cache, pokud origin server neodpovídá nebo má pomalou odezvu.
	+ V případě přetížení aplikačních serverů umožnit měnit režim provozu (viz kapitola 4).
* Vlastní konfiguraci a odpovědnost za její funkčnost je na straně Dodavatele. zadavatel zadává změnové požadavky pomocí podpory. Požadavky na změnu konfigurace jsou považovány za Běžný incident.
* Zadavatel má vždy v k dispozici aktuální konfiguraci Proxy Cache ve strojově i lidsky zpracovatelné/čitelné podobě.
* Cachování v RAM serveru kapacita 64 GiB
* Zasílání reálné IP adresy návštěvníka origin serveru (HTTP hlavičkou nebo PROXY protokolem)
* Možnost invalidace celé cache nebo části (podle URL požadavku nebo HTTP hlaviček odpovědi)
* Logování HTTP požadavků na úrovní Proxy Cache viz logování

### Aplikační server

* Fyzické nebo virtuální servery s rychlou možností rozšířit kapacitu RAM a počet jader procesoru.
* Rozšíření kapacity nebo počtu aplikačních serverů provádí Dodavatel nejpozději do 1 pracovního dne od doručení Objednávky nebo doručení dílčí smlouvy.
* Minimální počet aplikačních serverů je 4, každý obsahuje alespoň 4 jádra o taktu min. 3 GHz na 64 bitové architektuře Intel kompatibilní.
* Každý aplikační server obsahuje alespoň 32 GiB RAM.
* Výpočetní prostředky serveru (CPU, RAM) jsou vyhrazené pouze pro zadavatele.
* Každý aplikační server je schopen obsloužit alespoň 10 požadavků za sekundu na obvyklou Drupal stránku.
	+ Jako *obvyklá stránka* bude brána výchozí přihlašovací stránka /user
* PHP
	+ Verze 7.4 a vyšší
	+ Potřebná rozšíření (extensions) PHP jsou uvedeny v příloze *Současný technický stav.*
	+ Řešení musí umožnit budoucí přechod na novější verze PHP bez dalších nákladů.
* Pravidelně aktualizovaný webserver ve stabilní verzi, která není starší než 6 měsíců (pokud existuje novější), Web server musí být nginx, nebo Apache.
* 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.

### Databázový server

* Fyzické nebo virtuální servery s rychlou možností rozšířit kapacitu RAM a počet jader procesoru.
* Rozšíření kapacity nebo počtu databázových serverů provádí Dodavatel nejpozději do 3 pracovních dnů od doručení Objednávky nebo doručení dílčí smlouvy.
* Kompatibilní s MySQL 5.7 (např. Percona 5.6, MariaDB 10.3 ...)
* Řešení musí umožnit budoucí přechod na novější verze SQL serveru, podle aktuálních potřeb aplikace.
* Řešení umožňuje horizontální i vertikální škálování.
* Řešení bude provozováno v režimu s vysokou dostupností.
* Minimální počet databázových serverů je 3, každý obsahuje alespoň 4 jádra o taktu 3 GHz na 64 bitové architektuře Intel kompatibilní.
* Každý databázový server obsahuje alespoň 32 GiB RAM.
* Výpočetní prostředky serveru (CPU, RAM) jsou vyhrazené pouze pro zadavatele.
* 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.
* Zadavatel bude mít přístup k databázovému serveru pomocí dvou uživatelských účtů:
	+ Uživatel, který má právo čtení/zápisu/modifikace všech tabulek, přidávání/editace indexů, tabulek a views
	+ Uživatel s plným přístupem ke čtení všech dat a právem zápisu do dohodnuté množiny databázových tabulek (specifikace během realizace)
* Pro přístup k databázovým serverům bude k dispozici nástroj Adminer (vždy v aktuální verzi), přístupný pouze pomocí protokolu HTTPS
* K dispozici je “slow query log” (viz dále logování), na žádost je možné měnit konfiguraci long\_query\_time
* Všechna data jsou uložena na discích s parametry
	+ zápis > 30 000 iops, čtení > 50 000 iops
	+ zápis > 300 MiB/s, čtení > 400 MiB/s
* Zadavatel 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.
* Rozšíření kapacity je objednáváno jako navýšení dostupného prostoru a cena je vypočítána jako počet GiB x aktuální počet databázových serverů v clusteru.
* Přidání dalšího databázového serveru do clusteru je za jednotkovou cenu databázového serveru + poptávaná velikost RAM a počet CPU + aktuální kapacita úložiště v databázovém clusteru.

### Diskové úložiště pro statický obsah

* Společné úložiště přístupné ze všech aplikačních serverů.
* Připojení k aplikačním serverům alespoň 10 Gbps.
* Dvě úrovně rychlosti úložiště
	+ Pomalé pro velké statické soubory (typicky audio, video)
		- Výchozí kapacita 8 TiB, možnost okamžitého rozšíření kapacity
		- zápis > 200 iops, čtení > 250 iops
		- zápis > 100 MiB/s, čtení > 150 MiB/s
	+ Rychlé pro obrázky a další statický obsah, možnost okamžitého rozšíření kapacity
		- Výchozí kapacita 3 072 GiB
		- zápis > 10 000 iops, čtení > 15 000 iops
		- zápis > 250 MiB/s, čtení > 250 MiB/s
* Diskové úložiště podporuje tzv. snapshoty.
* Diskové úložiště je provozováno s redundancí na úrovni alespoň RAID6 nebo lepší.

### Paměťové úložiště (cache server)

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

### Server pro vyhledávání

* Jeden server Apache SOLR, pro účely vyhledávání obsahu v rámci administrace. V budoucnu na vyžádání zadavatele musí být dodavatel schopen nahradit SOLR server serverem Elaticsearch.
* Minimální kapacita 20 GiB.
* Aktuální zatížení a kapacita viz kapitola tohoto dokumentu *Současný technický stav.*
* Konfiguraci a správu vyhledávacího serveru provádí Dodavatel.

# Část C: Cloudová platforma mujRozhlas a další digitální produkty

## Současný technický stav

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

Přesný sizing lze nalézt v příloze “EXTERNAL - CRo infra analysis and sizing.xlsx”

Jako OS je použit Debian ve verzích 7-11, případně Ubuntu 18.

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

## Technické parametry virtualizované HW infrastruktury

Zadavatel požaduje cloudovou technologii VMware vCloud Director minimálně ve verzi 10.2. Nižší verze zadavatel nepřipouští z důvodů potencionálních problémů při migraci stávající infrastruktury.

Zadavatel 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.

|  |  |
| --- | --- |
| **parametr** | **hodnota** |
| **specifikace služby** | managed server hosting |
| **cloudová technologie (hypervisor)** | VMware vCloud Director min. verze 10.2 |
| **počet VM / vAPPs** | 128 / 32 |
| **Počet fyzických CPU jader** | 83 jader (CPU physical cores) o frekvenci alespoň 2,6 GHz (base clock) s možností zapnutí virtuálních jader (HTT, SMT atp.). |
| **vRAM (GB)** | 520 |
| **velikost úložiště (TB)** | 104 |
| **výkon úložiště dle účelu** | standardní / vysoký / špičkový |
| **Síť mezi VM** | min. 10 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) |

## 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) |

## Zálohování

Dodavatel bude automaticky vytvářet snapshoty běžících VM pomocí technologie Veeam a zálohovat je tak, aby mohl tyto zálohy použít i zadavatel pro obnovu VM mimo infrastrukturu dodavatele, především pak na prostředcích zadavatele. Vzhledem k tomu, že zadavatel 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.

Retence zálohování je minimálně 4 týdny.

## Konektivita

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

## Administrační rozhraní virtualizace

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.

## API virtualizace

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

## Výkonnostní požadavky

Řešení obslouží zátěž současné infrastruktury bez poklesu rychlosti – viz kapitola tohoto dokumentu *Současný technický stav.*

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

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

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.

# Obecné požadavky na datové centrum

## Redundance, architektura, propojení cloudů, lokality

**Požadavek na lokalitu a redundanci infrastruktury:**

* + 1. **Umístění jednotlivých částí cloudového prostředí:**
* Cloudová infrastruktura pro všechny tři části (Kubernetes, Drupal, mujRozhlas) **nesmí být soustředěna do jediné fyzické lokality/datacentra**.
* Minimálně jedna z částí (preferenčně platforma mujRozhlas nebo Kubernetes) musí být provozována **v jiné fyzické lokalitě**, než je hlavní produkční lokalita aplikačního cloudu.
	+ 1. **Redundance a provozní kontinuita:**
* Dodavatel musí zajistit **technickou i provozní redundanci** celé infrastruktury (výpočetní kapacita, úložiště, síťové prvky, atd.) v jiné geografické lokalitě, která není závislá na infrastruktuře hlavního datacentra.
* Požaduje se **aktivní nebo hot-standby zrcadlení** všech tří částí infrastruktury (Kubernetes, Drupal, mujRozhlas), které umožní:
	+ **přepnutí provozu** do záložního prostředí bez zásahu ČRo (max. výpadek 15 minut),
	+ plně automatizovaný failover pro vybrané kritické služby (Drupal, ArgoCD, Vault, databáze).
		1. **Disaster Recovery scénář:**
* Dodavatel musí navrhnout a realizovat **Disaster Recovery plán**, který zajistí obnovu všech tří částí cloudové infrastruktury v záložní lokalitě do 4 hodin od selhání primární lokality.
* Každé 3 měsíce bude provedeno failover testování s výstupem ve formě **auditovatelného reportu**.
	1. **Síťová propojenost lokalit:**
* Obě infrastruktury (primární a záložní) musí být propojeny **minimálně dvěma nezávislými datovými trasami** s propustností alespoň 1 Gbps.
* Musí být zajištěna možnost synchronizace dat mezi lokalitami v reálném čase nebo s maximálním zpožděním do 5 minut.
	1. **Soulad s legislativou a bezpečnostními normami:**
* Všechna řešení musí být v souladu s požadavky zákona č. 181/2014 Sb. o kybernetické bezpečnosti a vyhláškou NÚKIB č. 82/2018 Sb.
* Datová centra musí být minimálně TIER III dle Uptime Institute.
* Data ČRo nesmí opustit území ČR, pokud není výslovně uvedeno jinak.

## Požadavky na provoz

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

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

Produkční i testovací Infrastruktura umožňuje tři režimy provozu:

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

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

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

## Technické požadavky na produkční infrastrukturu

* + 1. **Dostupnost a provozní bezpečnost:**
* Dostupnost služeb produkčního prostředí musí dosahovat **minimálně 99,95 % ročně**.
* Produkční prostředí musí být umístěno v datovém centru s certifikací **minimálně TIER III** dle Uptime Institute (nebo doloženo čestným prohlášením).
	+ 1. **Redundance a spolehlivost:**
* Všechny klíčové komponenty produkčního prostředí (výpočetní kapacita, síťové prvky, úložiště) musí být provozovány v režimu minimálně **N+1**.
* Napájení a chlazení musí být rovněž plně redundantní, s garancí minimálně **72 hodin provozu při výpadku el. energie**.
	+ 1. **Výkon a rozšiřitelnost:**
* Výpočetní prostředky (CPU, RAM) musí být vyhrazené pro ČRo a musí umožnit **okamžité rozšíření výkonu** bez výpadku (min. do 24 hodin).
* Produkční prostředí musí zvládnout provoz podle aktuální zátěže specifikované v části 3, 4 a 5 technické dokumentace (Drupal: 400–550 req/s, Kubernetes: GitOps nástroje, mujRozhlas: více než 60 VM apod.).
	+ 1. **Síťová infrastruktura:**
* Konektivita minimálně **5 Gbps**, s **dvěma nezávislými optickými trasami** a přímou konektivitou do NIX.
* Interní propojení všech prvků produkční infrastruktury vyhrazenou **10 Gbps LAN**.
	+ 1. **Bezpečnost:**
* Přístup na fyzickou infrastrukturu jen pro autorizované osoby (2FA, kamerový systém, zabezpečený přístup).
* Ochrana DDoS (min. 1 Gbps s možností rozšíření), L4 firewall, IPS/IDS, WAF – dle kapitoly 6.10.
* Veškerá komunikace musí být šifrována (TLS, VPN WireGuard pro spojení s ČRo).
	+ 1. **Zálohování a obnova:**
* Zálohování musí probíhat minimálně **každé 2 hodiny (DB)** a **denně (disky)**.
* Zálohy musí být uchovávány dle požadavků v kap. 6.6 (30denních, 12 týdenních, 12 měsíčních).
* Obnova záloh musí být testována minimálně **1x ročně**, včetně fyzického testu LTO pásky v jiné lokalitě.
	+ 1. **Monitoring a provozní režimy:**
* Systém umožňuje sledování provozních metrik v reálném čase a alerting při překročení limitů.
* Produkční prostředí podporuje režimy:
	+ běžný provoz,
	+ provoz bez aplikačních serverů (proxy-only režim),
	+ krizový režim se statickou HTML stránkou.
		1. **Geo-redundance a failover:**
* V případě výpadku hlavního produkčního prostředí musí být k dispozici **záložní lokalita**, připravená k převzetí provozu do 15 minut (pro klíčové služby).
* Failover testy probíhají kvartálně, výstupy musí být archivovány pro audit.
	+ 1. **Omezení:**
* Veškerá data musí být fyzicky uložena **na území České republiky**, pokud není výslovně uvedeno jinak.

## Technické požadavky na testovací infrastrukturu

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

## Požadavky na publikování aplikací (deploy)

Možnost provádění publikaci skrze robustní workflow – prostřednictvím jedné akce / příkazu (s potvrzením) je možné provést deploy kódu na všechny aplikační servery.

Deploy na aplikační servery musí být možný i pomocí Deployer z prostředí Bitbucket pipeline

Jde tedy o zpřístupnění webserverů via SSH z IP adres Bitbucketu

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

Je možné spouštět drush příkazy.

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

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

## Monitoring a alerting

Následující metriky má zadavatel online přístupné v podobě denních, týdenních, měsíčních a ročních grafů:

* Vytížení internetové konektivity
* Počet všech HTTP požadavků za sekundu, rozlišené podle požadavků, které byly/nebyly obsloužené z cache.
* Počet HTTP požadavků na stránky (tedy mimo assety) za sekundu, rozlišené podle požadavků, které byly/nebyly obsloužené z cache.
* Zátěž load balanceru
* Zátěž proxy cache
* Zaplnění proxy cache
* Počet požadavků na aplikační servery za sekundu.
* Zátěž aplikačních serverů
* Počet databázových dotazů za sekundu s rozlišením podle druhu
* Zátěž databázových serverů
* Počet požadavků na paměťové úložiště za sekundu s rozlišením hit/miss.
* Zaplnění paměťového úložiště
* Vytížení LAN
* Vytížení diskového úložiště
* Zaplnění diskového úložiště

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).

**Příklad sledovaných metrik, nejedná se o kompletní výčet:**

* Load balancer (počet požadavků, load)
* Reverzení proxy cache (počet požadavků, hits, misses, zaplnění cache, počet objektů)
* Aplikační server - pro každou instanci (počet požadavků, požadavky podle stavového kódu odpovědi, běhové chyby, load jednotlivých serverů)
* Databázovy servery (load, počet dotazů za vteřinu a jejich typy)
* Paměťové úložiště - pro každou instanci (počet požadavků hits, misses, zaplnění cache, počet objektů)

**Příklad otázek, na které zadavatel chce znát odpověď:**

* Graf poměru návštěvnosti z vyhledávačů pro doménu XY za období AB.
* Průměrná doba renderování necachované URL za den

**Příklad filtrů (a jejich kombinací), které chceme používat**

* Časové období OD-DO
* Domény (1 - všechny)
* Požadavek ne/obsloužen z proxy cache
* Ne/přihlášený uživatel (podle cookie)
* Crawler/normální návštěvník (podle UA)
* Filtrování v názvu URL

Stav a zátěž a využití kapacity infrastruktury, a odezva určených URL je automaticky monitorována vhodným systémem (např. Icinga 2).

Pro monitorované hodnoty (SLI) jsou dohodou určeny příslušné hranice (SLO) při jejichž překročení je zadavatel dohodnutým způsobem (mail, Slack, Pagerduty…) notifikován.

## Zálohování

* 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
* Záloha databáze se provádí každé dvě hodiny a je uchováno posledních 30 dní záloh.
* Jedna denní záloha je konzistentní s příslušnou zálohou souborových dat.
* Prováděné zálohování neovlivňuje výkon ani funkce řešení.
* Zadavatel má zajištěn přímý přístup k zálohám. Formát, způsob a orientační časová náročnost obnovy záloh je dokumentována.
* Zadavatelem vymezený rozsah záloh je v dohodnutých intervalech synchronizován na prostředky zadavatele pomocí dohodnutého a šifrovaného protokolu sítě internet.

Fyzické offline zálohování bude probíhat na LTO pásky 8 nebo 9 pro celé datacentrum ČRO, na půlroční bázi. Přičemž pásky budou uchovány v utěsněném a ohnivzdorném trezoru dodavatele, který bude v jiné lokalitě, čímž se rozumí minimálně jiná budova. Nácvik obnovy pásek bude probíhat ročně pro splnění potřebných norem včetně všech souvisejících pravidel relevantních pro dotčenou organizaci.

Provozovatel datového centra ve spolupráci s ČRo vytvoří politiku pro pravidelné aktivní využívání a testování záloh za účelem ověřování integrity a funkčnosti dat.

**Testovací scénář:**

* Návrh provede dodavatel a po odsouhlasení ČRO provede exekuci.
* Scénář by měl obsahovat následující kroky
	+ Restore operation, konkrétní definice jaká data se budou obnovovat bude navržen Dodavatelem včetně odůvodnění, proč byla konkrétní část vybrána.
	+ Ověření dat
	+ Report, který bude uchován pro případnou kontrolu

## Logování

* Všechny HTTP požadavky na infrastrukturu jsou logovány a agregovány na úroveň jednotlivého HTTP požadavku s ukládáním informací minimálně v rozsahu NCSA combined.
* U požadavků z origin serverů je logována doba zpracování požadavků na origin serveru.
* Dočasně a na vyžádání (pro účely ladění) je možné do logu ukládat HTTP hlavičky z odpovědi origin serveru.
* K dispozici jsou na jednom místě agregované PHP error logy ze všech origin serverů, s logováním na úrovni Notice.
* K dispozici je MySQL slow query log
* Na vyžádání je možné zapnout zaznamenávání MySQL query logu po dobu až 24 hodin.
* K dispozici je Drupal log, s parametry jako PHP error log. Drupal log není ukládán do MySQL databáze Drupalu.
* Error log PHP a log Drupalu je k dispozici v reálném čase, všechny ostatní logy jsou k dispozici se zpožděním maximálně 5 minut.
* 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)
* Všechny logy jsou rotovány po dnech a logicky pojmenovány tak, aby je bylo možné automaticky zpracovávat.
* Logy jsou uchovávány za posledních 12 měsíců.
* Úložiště logů není dodatečně zpoplatněno nad základní cenu řešení.

## Provozní požadavky na datacentra a zapojení serverů

Za účelem garance vysoké dostupnosti služeb datového centra zadavatel 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:

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

Dostupnost služeb datového centra musí dosahovat alespoň 99,95 % ročně, viz SLA.

Připojení serverů na alespoň dvě nezávislé větve napájení kdy výpadek jedné libovolné větve nijak neomezí provoz serverů.

V případě HA clusteru virtuálních serverů, musí být každý virtuální server na vlastním HW, tak aby případná HW porucha neovlivnila celý cluster

* Dostupnost služeb datacentra alespoň 99.95 % ročně
* Garantováno minimálně 72 hodin provozu při výpadku el. energie
* Minimálně 2 dieselgenerátory
* Redundance všech komponent alespoň N+1
* Redundantní chlazení
* Protipožární systém, automatický hasící systém
* Přístup na datový sál pomocí dvou faktorů (čip / biometrika, čip / PIN, klíč / pin, …)
* Kamerový systém s uchováváním záznamů
* K infrastruktuře nemají přístup jiné osoby, než pověřené Dodavatelem
* Minimálně 2 nezávislé optické trasy konektivity
* Přímá konektivita do NIX
* Neomezený datový přenos v rámci ČR i mimo ČR.
* Konektivita minimálně 5 Gbps bez ohledu na použitou trasu.
* Použito IPv4 i IPv6.
* Servery a síťové prvky propojeny vyhrazenou LAN 10 Gbps
* Celá infrastruktura a procesy dodavatele jsou připraveny na to, že zadavatel může potřebovat předřadit celému řešení jednu popř. více proxy (ať už od dodavatele, svoje či třetí strany).
	+ Nasazení takovýchto proxy je možné zvlášť pro testovací i produkční prostředí.
	+ Dodavatel upraví konfigurace do 30 dnů po sdělení objednatele, že má v plánu takové řešení nasadit. Zadavatel sdělí dodavateli IP adresy nebo URL kde jsou k dispozici IP adresy těchto proxy a jak často je třeba seznam aktualizovat.
	+ Před faktickou aktivací proxy (typicky změnou DNS záznamů) zadavatel informuje o přesném datu a času přepnutí minimálně 3 pracovní dny předem. Aktivaci proxy může zadavatel provést až po potvrzení dodavatele, že je konfigurace infrastruktury na přepnutí připravena.
	+ Řešení počítá s tím, že původní IP adresa uživatele bude v případě HTTP(S) protokolu v zadavatelem specifikované HTTP hlavičce v obvyklém formátu. Tuto IP adresu řešení dále propaguje až k aplikačnímu serveru tak, aby byla aplikacím zadavatele k dispozici a současně ji ukládá do všech logů, které ukládají IP adresu klienta.

## Bezpečnostní požadavky

### DDoS ochrana

* 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.
* 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.
* Ochrana na ISO/OSI vrstvě 3 a 4 (ochrana sítě) je implementována minimálně na úrovni celého datacentra nebo (lépe) u poskytovatelů připojení datacentra.
* Ochrana na ISO/OSI vrstvě 7 (ochrana serveru) chrání minimálně protokol HTTP.
* Ochrana eliminuje útoky až do 1 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).
* Ochrana umožňuje výrazné omezení nebo úplného odříznutí mezinárodního provozu (požadavků přicházejících mimo ČR)
* Možnost úprav a nastavení vlastních pravidel a limitů pro detekci a prevenci útoků na základě žádosti zadavatele včetně explicitního whitelistingu/blacklistingu.
* V případě detekovaného útoku je zadavatel o této skutečnosti neprodleně notifikován včetně podrobností o útoku a přijatých opatřeních. Během probíhajícího útoku je pak pravidelně informován o aktuálním stavu.
* Součástí měsíčních reportů jsou detailní informace o zachycených útocích.
* 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.

### Ochrana IPS/IDS pro detekci a prevenci dalších typů útoků

* databáze pravidel se automaticky aktualizuje
* systém vidí do kompletního síťového provozu
* jednotlivá pravidla lze dynamicky vypínat / zapínat
* pro jednotlivá pravidla lze nastavit zda se mají aplikovat v režimu IDS (pouhá detekce) nebo IPS (blokování)
* dodavatel nacení řešení pro minimálně 1 Gbps ingress provozu
* zadavatel zváží nasazení IPS/ IDS dle evaluace přínosů vs. nákladů (viz vyhrazená změna závazku), tj. nacenění výše se nezapočítává do nabídkové ceny

### L4 Firewall

* + - Možnost blokace definovaných cílových portů (TCP i UDP)
		- Možnost blokace ICMP
		- Možnost blokace na základě sítě či IP adresy zdroje či cíle

### Webový Aplikační firewall (WAF)

* Automaticky aktualizovaná pravidla, minimálně OWASP core a pravidla specifická pro Drupal.
* Možnost vlastních pravidel a deaktivace / konfigurace všech pravidel
* Detekce robotů (legitimních i nelegitimních)
* Různé možnosti reakce, minimálně:
* Blokace
* Omezení rychlosti (rate-limiting)
* Logování
* dodavatel nacení řešení jako cenu za milion prozkoumaných HTTP(S) požadavků
* zadavatel zváží nasazení WAF dle evaluace přínosů vs. nákladů (viz vyhrazená změna závazku), tj. nacenění výše se nezapočítává do nabídkové ceny

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 HTTP hlavičkou nebo PROXY protokolem.

## Dokumentace

Veškerá́ zmíněná dokumentace je v češtině nebo angličtině.

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

Kompletní uživatelská i správcovská dokumentace všech komponent, které jsou součástí řešení

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

## Licence

Všechny komponenty Infrastruktury jsou provozovány bez licenčních poplatků ze strany zadavatele.

zadavatel prefereruje použití open-source software, na jeho použití trvá u komponent:

* Aplikační server (webserver)
* Databázový server
* Paměťové úložiště (cache server)
* Server pro vyhledávání

## Podpora a údržba

Povinnosti dle specifikace smlouvy.

## Organizační požadavky

* 1x měsíčně povinnost účasti (osobně nebo online) na stand-up schůzce svolané zadavatelem, kde bude možné řešit směry dalších úprav/optimalizací infrastruktury a stav prací na zadaných požadavcích.
* měsíční vykazování hodin týkajících se servisní podpory a plnění požadavků zadavatele

## Milníky

* dodání virtualizované HW infrastruktury připravené pro migraci stávající infrastruktury, migraci dat a testování – nejpozději do 2 týdnů od účinnosti 1. dílčí smlouvy;
* dokončení migrace stávající infrastruktury včetně middleware a aplikační vrstvy a uvedení cloudu do plného provozu – nejpozději 4 týdny od účinnosti 1. dílčí smlouvy.
* Spuštění ostrého provozu: prosinec 2025

## Migrace

Zadavatel požaduje provedení případné migrace stávající infrastruktury od stávajícího dodavatele bez dopadu na služby zadavatele provozované v současné infrastruktuře. Za tímto účelem je dodavatel povinen koncipovat migraci jako bezvýpadkovou. Migrace může probíhat po jednotlivých službách.

Migrace buide provedena bezvýpadkově dle postupu níže, před započetím následujících fází je potřeba optimalizovat využití zdrojů a odstavit nepoužívané VMs dle specifikace. Poté přejít k následujícím obecným fázím:

**1. Fáze** “Migrace k novému Cloud dodavateli nebo na novou infrastrukturu (Lift and shift)”

**2. Fáze** “Převedení databáze původního řešení do nových manažovaných databází”

**3. Fáze** “Migrace workloadu z VMs do Kubernetes”

Detailní popis migrace je uveden v Příloze číslo 1 tohoto dokumentu “Požadavky na migraci”. **Pro vyloučení pochybností je Dodavatel povinen zajistit kompletní proces migrace popsaný v příloze číslo 1 tohoto dokumentu.**

Dodavatel předloží zadavateli harmonogram migrace a se zadavatelem určí datum, kdy bude k dispozici kopie produkčního prostředí. Za účelem sestavení harmonogramu zadavatel dodá seznam všech služeb a jejich provázanost. Součástí bude i vazba konkrétních aplikací na konkrétní jednotlivé databáze (kvůli přenosu dumpů). Dodavatel zajistí všechny další potřebné kroky migrace kromě přepnutí DNS.

## **PŘÍLOHA č. 1 – POŽADAVKY NA MIGRACI**

## **1. Úvod a účel**

Tento dokument specifikuje minimální požadavky na způsob provedení migrace aplikačního a datového stacku služby při přechodu na nového dodavatele cloudových služeb.

Požadavky vycházejí z potřeb zajištění kontinuity provozu, minimalizace rizik ztráty dat a souladu s předpisy kybernetické bezpečnosti platnými pro Český rozhlas.

**2. Specifické technické požadavky na migraci**

#### **2.1 Primární metoda migrace dat**

a) **Primární přenos dat (bulk transfer) musí být realizován prostřednictvím fyzických mobilních diskových polí** (např. RAID/NAS/JBOD boxů), na které budou z původního datového centra exportována aktuální data (diskové image, zálohy databází, soubory aplikace).

b) Disková pole musí být kompatibilní s technologií cílového datového centra a umožnit přímý import dat do virtualizační platformy nebo storage clusteru dodavatele.

#### **2.2 Šifrování a ochrana dat**

a) **Disková pole musí být šifrována** na úrovni celého svazku pomocí technologií jako LUKS (Linux Unified Key Setup) nebo Microsoft BitLocker.

b) Dodavatel předloží návrh postupu šifrování včetně způsobu správy šifrovacích klíčů a bude garantovat, že data zůstanou chráněna proti přístupu neoprávněných osob po celou dobu transportu.

#### **2.3 Transport a chain-of-custody**

a) Transport diskových polí bude realizován certifikovanou logistickou společností nebo jiným způsobem schváleným zadavatelem.

b) Dodavatel zajistí **dokumentovaný „chain-of-custody“ proces**, který bude zahrnovat minimálně:

* evidenci předání a převzetí diskových polí,
* záznam o zapečetění a otevření obalů,
* datum a čas exportu a importu dat.

#### **2.4 Doplňková synchronizace změn (delta sync)**

Po provedení primárního fyzického přenosu dat bude realizována **doplňková synchronizace (delta sync) prostřednictvím zabezpečeného připojení (VPN/IPSec)**, za účelem dorovnání datových změn vzniklých od okamžiku fyzického exportu po okamžik přepnutí provozu (cutover).

#### **2.5 Cutover a omezení výpadku**

a) Přepnutí provozu aplikace do nového prostředí (cutover) bude provedeno s minimalizovaným výpadkem, jehož maximální doba bude předem dohodnuta a specifikována ve smlouvě SLA.

b) Po cutover bude provedeno ověření funkčnosti služby prostřednictvím integračních a sanity testů.

#### **2.6 Harmonogram, rollback a reporting**

a) Dodavatel předloží podrobný **harmonogram migračních kroků**, včetně identifikace všech závislostí a navržených kontrolních bodů.

b) Součástí plánu bude i **rollback scénář**, který umožní bezpečný návrat do původního prostředí v případě zjištění kritických problémů během nebo bezprostředně po cutover.

c) Po úspěšné migraci bude dodavatelem vypracována a předána **migrační zpráva**, obsahující přehled provedených kroků, záznamy z chain-of-custody, výsledky testů funkčnosti a doporučení pro další provoz.

d) Migrace musí být úspěšně provedena nejpozději do první poloviny prosince 2025. Od tohoto termínu se předpokládá produkční spuštění dodané serverové infrastruktury.

#### **2.7 Soulad s právními a bezpečnostními předpisy**

a) Celý migrační proces musí být realizován v souladu s:

* požadavky zákona č. 181/2014 Sb., o kybernetické bezpečnosti,
* vyhláškou NÚKIB č. 82/2018 Sb.,
* relevantními ustanoveními GDPR,
* interními bezpečnostními politikami Českého rozhlasu.

**3. Požadované metriky SLA během migrace**

|  |  |
| --- | --- |
| **Metrika** | **Hodnota / podmínka** |
| Maximální downtime | dle dohody, předběžný cíl max. **4 hodiny** |
| Maximální RPO | **< 1 hodina** (po synchronizaci delta sync) |
| Doba dodání migr. plánu | do **14 dnů od podpisu smlouvy** |

# Přílohy

• Příloha A – Seznam zkratek a definic použitých v dokumentu

• Příloha B – Topologie a architektura cloudové infrastruktury

• Příloha C – SLA metriky a akceptační kritéria

**Příloha A – Seznam zkratek a definic použitých v dokumentu**

ČRo – Český rozhlas

SLA – Service Level Agreement (Dohoda o úrovni služeb)

DR – Disaster Recovery (Obnova po havárii)

VM – Virtuální stroj

K8s – Kubernetes

CI/CD – Continuous Integration / Continuous Deployment

MFA – Multi-Factor Authentication

IAM – Identity and Access Management

NIX – Neutral Internet eXchange (český peeringový uzel)

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

ArgoCD – GitOps nástroj pro správu Kubernetes deploymentů

Vault – Nástroj pro správu tajemství (např. hesel, tokenů, certifikátů)

Prometheus – Open-source nástroj pro sběr a zpracování metrik

Grafana – Nástroj pro vizualizaci metrik a stavů systému

**Příloha B – Topologie a architektura cloudové infrastruktury**

Cloudová infrastruktura se skládá ze tří hlavních vrstev:

1. Kubernetes platforma – slouží pro provoz kontejnerizovaných aplikací dle GitOps principů.

2. Aplikační cloud pro Drupal – hostuje CMS systém s vysokou dostupností a škálovatelností.

3. Platforma mujRozhlas – provozována na VM infrastruktuře, napojená na vlastní databázové a cache služby.

Infrastruktura musí být fyzicky oddělena do dvou geograficky separovaných lokalit (primární a záložní).

Každá lokalita musí obsahovat kopii všech tří částí prostředí.

Mezi lokalitami musí být zajištěno síťové propojení (min. 2x 1 Gbps) a synchronizace dat s maximální latencí 5 minut.

**Příloha C – SLA metriky a akceptační kritéria**

Minimální garantovaná dostupnost produkčního prostředí: 99,95 % ročně

Reakční doba na kritický incident: max. 15 minut (24/7)

Doba vyřešení kritického incidentu: max. 4 hodiny

Testování záloh: minimálně 1× ročně (včetně fyzického testu obnovy)

Monitoring a alerting: plně automatizovaný, se záznamem všech incidentů

Reporting: měsíční přehled SLA splnění, alertů a provozních statistik