BH TELECOM

ZAHTJEV ZA INFORMACIJAMA (RFI)

Telco Cloud referentna arhitektura

Kontejnerska platforma za telco aplikacije (CNF)

Sarajevo, novembar 2026.

SADRŽAJ

SLUŽBENI PROPRATNI DOPIS (ZA DOBAVLJAČE INFRASTRUKTURE I PONUĐAČE USLUGA) 4
1. UVOD I STRATEŠKI CILJ PROJEKTA 5
2. TEHNIČKI UPITNIK 7
2.1. Zahtjevi platforme i CNF-ova prema fizičkom hardveru 7
2.2. Sloj kontejnerizacije i Kubernetes platforme (CaaS/PaaS) 8
2.3. Mrežna infrastruktura, sinhronizacija i topologija 10
2.4. Pohrana podataka i upravljanje stanjem 11
2.5. Sigurnost i hardening platforme 11
2.6. Upravljanje životnim ciklusom, automatizacija i rad sa više klastera 12
2.7. Visoka raspoloživost, kontinuitet poslovanja i oporavak od katastrofe (HA, BC/DR) 13
2.8. Hardver i mrežna oprema – ponuda dobavljača 14
Virtuelizacija kao opcionalna varijanta platforme: 15
3. MATRICA TEHNIČKIH PREDUSLOVA 15
3.1. Matrica – Telco Cloud referentna arhitektura (kontejnerska platforma) 16
3.2. Detaljna izjava o usklađenosti (SoC) 18
4. USLOVI ZA POTPUNU PODRŽANOST I RAZGRANIČENJE ODGOVORNOSTI 18
4.1. Certifikacija i usklađenost s otvorenim standardima 18
4.2. Razgraničenje odgovornosti i validacija 19
4.3. Multi-App Hosting & Isolation 20
4.4. Ops & Observability 20
4.5. Podrška, životni ciklus i suverenitet 21
4.6. Onboarding, integracija i upravljanje životnim ciklusom CNF-ova u multi-vendor okruženju 21
4.7. Dokazi i prateća dokumentacija 22
4.8. Komercijalne informacije i indikativne cijene 23
PRILOG 1 – DETALJNA IZJAVA O USKLAĐENOSTI (SoC): ZAHTJEVI ZA TELCO-GRADE KUBERNETES PLATFORMU 24
PRILOG 2 – OBRAZAC ZA INDIKATIVNE CIJENE 34

SLUŽBENI PROPRATNI DOPIS (ZA DOBAVLJAČE INFRASTRUKTURE I PONUĐAČE USLUGA)

Predmet: Zahtjev za informacijama (RFI – Request for Information) – Tehnički uslovi, usklađenost i spremnost infrastrukture za Cloud-Native softverska rješenja.

Kompanija BH Telecom je u procesu strateškog planiranja i transformacije svoje mrežne infrastrukture prema modernom, otvorenom i cloud-native okruženju. Naš dugoročni cilj je izgradnja agnostičke i fleksibilne mikroservisne platforme temeljene na Kubernetesu, koja će biti sposobna podržati kritične telekomunikacijske servise (prvenstveno 5G Core), kao i druga napredna cloud-native rješenja.

Polazište ovog RFI-ja je **Telco Cloud referentna arhitektura**, s fokusom na kontejnersku (Kubernetes) platformu namijenjenu instalaciji i izvršavanju telekomunikacijskih aplikacija (CNF – Cloud-Native Network Functions) različitih proizvođača. Cilj je sagledati različite mogućnosti implementacije platforme, uključujući pripadajuću hardversku i softversku infrastrukturu, te utvrditi optimalnu arhitekturu koja će osigurati interoperabilnost, skalabilnost, performanse, stabilnost i punu podržanost rješenja u multi-vendor okruženju.

Kako bismo izbjegli ovisnost o pojedinačnim dobavljačima (vendor lock-in) te osigurali dugoročnu fleksibilnost i održivost budućeg rješenja, provodimo sveobuhvatno istraživanje tržišta. Ovim RFI-jem želimo prikupiti i uskladiti informacije od **dobavljača hardvera i mrežne opreme**, s jedne strane, te **ponuđača softverskih rješenja i usluga**, s druge strane, kako bismo sagledali mogućnosti integracije svih komponenti i utvrdili optimalnu tehničku arhitekturu budućeg Telco Cloud okruženja.

U nastavku ovog dokumenta nalazi se cjeloviti zahtjev za informacijama u kojem su detaljna pitanja i tehnička matrica koja se odnosi na:

1. **Zahtjeve softverskih rješenja** prema fizičkom hardveru (COTS) i hardverskim mogućnostima koje dobavljači opreme mogu isporučiti.
2. **Potrebne napredne mrežne i infrastrukturne preduslove** na nivou Kubernetes platforme (CNI, SR-IOV, DPDK, CPU Pinning itd.).
3. **Uslove i granice odgovornosti** za pružanje službene tehničke podrške u multi-vendor okruženju.
4. **Sigurnost, hardening, nadzor i upravljanje životnim ciklusom** kontejnerske platforme, uključujući detaljnu izjavu o usklađenosti (SoC – Statement of Compliance) datu u Prilogu 1.
5. **Visoku raspoloživost, kontinuitet poslovanja i oporavak od katastrofe**, model onboardinga i integracije CNF-ova u multi-vendor okruženju, te komercijalne informacije (indikativne cijene i modeli licenciranja).

Vaši odgovori, iskustva i stručni prijedlozi pomoći će nam da precizno definišemo arhitekturu i tehničke specifikacije za nadogradnju naše interne platforme, kako bi ona bila potpuno spremna za savremena telekomunikacijska rješenja. Sve upite ili nejasnoće molim da adresirate na cloud.podrska@bhtelecom.ba kao i na ostale korespondencijske kanale definsane kroz objavu RFI.

ZAHTJEV ZA INFORMACIJAMA (RFI)

Multi-Vendor Cloud-Native rješenje: Tehnički uslovi i spremnost infrastrukture

Telco Cloud referentna arhitektura - kontejnerska platforma za telco aplikacije (CNF)

1. UVOD I STRATEŠKI CILJ PROJEKTA

BH Telecom provodi istraživanje tržišta usmjereno prema dobavljačima opreme i ponuđačima softverskih usluga s ciljem izgradnje moderne, otvorene i napredne infrastrukture temeljene na mikroservisima i Kubernetesu.

Cilj ovog RFI-ja je definisati tačne hardverske, mrežne i softverske preduslove koje naša platforma mora ispuniti kako bi bila u potpunosti podržana za kritične telekomunikacijske servise (5G Core) kao i sva ostala napredna cloud-native rješenja.

BH Telecom teži eliminaciji vendor lock-in-a i stvaranju univerzalnog infrastrukturnog Compute Pool-a sposobnog za sigurno i stabilno prihvatanje rješenja s obje strane. Želimo osigurati da se bilo koje ponuđeno softversko rješenje može besprijekorno instalirati na COTS platformu osiguranu od strane naših dobavljača opreme, uz punu službenu podršku svih strana, bez nametanja zatvorenih ekosistema.

Zahtjevi ovog RFI-ja podijeljeni su strukturalno na sljedeći način:

- **Telco Cloud referentna arhitektura (kontejnerska platforma za telekomunikacijske aplikacije):** zahtjevi za kontejnersku platformu (CaaS – Container as a Service), namijenjenu instalaciji i izvršavanju telekomunikacijskih aplikacija (CNF) različitih proizvođača – poglavlja 2.1 do 2.8, matrica tehničkih preduslova (poglavlje 3.1), detaljna izjava o usklađenosti (poglavlje 3.2 i Prilog 1), te poglavlja 4.1 do 4.8 (podržanost i odgovornosti, onboarding CNF-ova, dokazi i komercijalne informacije).
- **Opcionalno – Virtuelizacijska platforma:** platforma na kojoj se izvršavaju virtuelne mašine (VNF, postojeći i prateći sistemi). Informacije se dostavljaju u slobodnoj formi, kako je opisano u odjeljku „Virtuelizacija kao opcionalna varijanta platforme“ na kraju poglavlja 2, i nisu uslov za ocjenu usklađenosti.

Vodeći principi Telco Cloud referentne arhitekture

Od ponuđača se očekuje da predložena rješenja budu usklađena sa sljedećim principima, te da za svaki od njih obrazlože način ispunjavanja zahtjeva i opišu relevantne tehničke mogućnosti kojima se osigurava njihova primjena:

- **Horizontalna platforma:** jedna zajednička kontejnerska platforma za CNF-ove više proizvođača (5G Core, signalizacija, IMS, upravljanje pretplatničkim podacima, OSS/BSS i dr.), umjesto vertikalnih silosa u kojima svaki proizvođač aplikacije isporučuje vlastitu platformu.

- **Fleksibilnost modela implementacije:** Očekuje se da ponuđači predstave podržane modele implementacije kontejnerske platforme, uključujući instalaciju direktno na fizičkim serverima (bare-metal), implementaciju na virtualizacijskoj infrastrukturi, kao i hibridne modele. Za svaki ponuđeni model potrebno je opisati arhitekturu, performanse, skalabilnost, ograničenja, zahtjeve za hardverom i model tehničke podrške. Posebno je potrebno obrazložiti preporučeni model implementacije za kritične telekomunikacijske servise.
- **Open-source tehnologije, otvoreni standardi i interoperabilnost:** Platforma treba biti zasnovana na open-source projektima i otvorenim, standardnim interfejsima (CNCF-conformant Kubernetes API, CNI, CSI, OCI), uz usklađenost s relevantnim preporukama i standardima CNCF-a, GSMA/Anuket, ETSI NFV i 3GPP. Aktivan doprinos proizvođača upstream zajednicama smatra se prednošću, ali nije uslov. Ukoliko platforma nije u cijelosti zasnovana na open-source projektima, potrebno je dostaviti relevantnu tehničku dokumentaciju.
- **Jedinstven životni ciklus i jedna tačka podrške:** Preferira se model u kojem su operativni sistem čvorova, Kubernetes i platformske usluge (mreža, pohrana, nadzor, registar, sigurnost) isporučeni, testirani, nadograđivani i podržani kao jedinstvena cjelina od strane jednog proizvođača. Ukoliko ponuđeno rješenje uključuje komponente različitih proizvođača, potrebno je detaljno opisati model isporuke, održavanja i podrške, jasno definisati granice odgovornosti i predložiti mehanizam koordinacije podrške između uključenih proizvođača (back-to-back model).
- **Deklarativno upravljanje i automatizacija:** instalacija, konfiguracija i nadogradnja platforme i CNF-ova vođeni kodom (GitOps, Operator obrazac, Infrastructure-as-Code), sa centralnim upravljanjem više klastera od core do edge lokacija.
- **Sigurnost po dizajnu:** platforma se isporučuje u ojačanom (hardened) stanju, sa restriktivnim zadanim postavkama i dokazivom usklađenošću sa priznatim sigurnosnim standardima.
- **Opcionalno: konvergencija kontejnera i virtuelnih mašina:** mogućnost da se, gdje je to opravdano, virtuelne mašine i kontejneri izvršavaju i njima upravlja na istoj platformi, istim alatima i uz isti model podrške.

2. TEHNIČKI UPITNIK

Molimo da na pitanja i tehničku tablicu odgovorite iz perspektive vaše domene (bilo da ste dobavljač infrastrukturne/mrežne opreme ili ponuđač softverskih servisa/aplikacija). Nije potrebno odgovoriti na pitanja koja se ne odnose na vašu domenu; takva pitanja označite kao „nije primjenjivo". Djelimični odgovori, kao i zajednički odgovori više partnera (npr. proizvođač hardvera i proizvođač platforme), dobrodošli su i neće se smatrati nedostatkom. Za svaki zahtjev navesti da li je ispunjen standardnom funkcionalnošću platforme, dodatnom (third-party) komponentom ili je planiran u budućim verzijama.

TELCO CLOUD REFERENTNA ARHITEKTURA: KONTEJNERSKA PLATFORMA ZA TELEKOMUNIKACIJSKE APLIKACIJE (CNF)

Poglavlja 2.1 do 2.7 odnose se na kontejnersku platformu namijenjenu instalaciji i izvršavanju telco aplikacija (CNF) različitih proizvođača. Od dobavljača platforme očekuje se da opišu način na koji platforma ispunjava navedene zahtjeve, dok se od ponuđača telco aplikacija očekuje da navedu zahtjeve koje njihove aplikacije postavljaju prema kontejnerskoj platformi

Poglavlje 2.8 namijenjeno je opisu ponuđene serverske i mrežne opreme, njenih tehničkih karakteristika, mogućnosti integracije i validacije sa različitim kontejnerskim platformama i CNF rješenjima, kao i modela podrške i upravljanja životnim ciklusom opreme.

2.1. Zahtjevi platforme i CNF-ova prema fizičkom hardveru

Cilj nam je nabaviti standardni, komercijalno dostupni (COTS) hardver koji može pokrenuti kritične servise uz maksimalne performanse.

- **Podržane procesorske arhitekture:** Detaljno opisati procesorsku arhitekturu rješenja (x86 arhitektura (Intel/AMD) ili ARM), uključujući eventualna ograničenja i razlike u funkcionalnosti i performansama između arhitektura.
- **Specifične procesorske instrukcije:** Zahtijevaju li kritične funkcije specifične procesorske instrukcije, odnosno može li oprema koju nudite isporučiti takve performanse?
- **Hardware Offloading:** Koristi li vaše softversko rješenje – odnosno podržava li vaša mrežna/serverska oprema – hardware offloading za kriptografiju ili naprednu obradu paketa na mrežnoj razini (npr. SmartNIC, DPU/IPU)?
- **Optimizacija memorije i CPU jezgri:** Opisati referentnu arhitekturu i osjetljivost aplikacija na NUMA (Non-Uniform Memory Access) arhitekturu, te navesti da li se, radi sprječavanja latencije, zahtijeva ekskluzivno dodjeljivanje CPU jezgri (CPU Pinning) i zaključavanje memorije (Huge Pages).
- **Model instalacije i podržani hardver:** Opisati podržane modele implementacije kontejnerske platforme, uključujući instalaciju direktno na fizičke servere (bare-metal), implementaciju na virtualizacijskoj infrastrukturi (putem posredujućeg hipervizora), kao i mogućnost primjene hibridnog modela. Navesti mogućnosti automatizovanog uvođenja i konfiguracije infrastrukture (bare-metal provisioning), te dostaviti listu certificiranih i službeno podržanih servera i mrežnih kartica različitih proizvođača hardvera.

- **Profili čvorova (node pools):** Opisati podršku za formiranje više grupa čvorova sa različitim hardverskim profilima (opšti, high-performance, storage-optimizovani), raspoređivanje CNF-ova na odgovarajuće profile putem labela i selektora, kao i kontrolu raspoređivanja i izolaciju grupa čvorova korištenjem Taints/Tolerations mehanizama i drugih odgovarajućih mehanizama platforme.
- **Izolacija jezgri i real-time rad:** Opisati podršku za izolaciju CPU jezgri na nivou operativnog sistema (isolcpus, nohz_full, rcu_nocbs) i korištenje real-time kernela na radnim čvorovima, te način na koji se ove postavke primjenjuju i održavaju kroz nadogradnje (deklarativno, putem platforme, bez ručnih izmjena na čvorovima).
- **Minimalne karakteristike procesora i memorije:** Navesti preporučene modele procesora, broj CPU jezgri, bazni i turbo takt, generaciju memorije (DDR4/DDR5) i minimalne zahtijevane performanse po jezgri za podržani rad aplikacija. Vrijednost od 2,4 GHz smatra se okvirnom referentnom vrijednošću, dok se konačni zahtjevi definišu prema preporukama proizvođača softverskog rješenja.
- **Redundansa i fizičko razdvajanje:** Opisati preporučenu fizičku i logičku mrežnu topologiju, uključujući redundantne mrežne putanje između čvorova i ToR (Top-of-Rack) switch-eva (LACP ili ekvivalentni mehanizmi), fizičko ili logičko (VLAN) razdvajanje management, underlay, storage i CNF data-plane mreža, te preporučeni raspored čvorova po rack-ovima i zonama dostupnosti (Availability Zones).
- **Upravljanje serverima i nadzor hardvera:** Opisati mogućnosti upravljanja serverima i nadzora hardverskih komponenti putem otvorenih standardnih interfejsa (DMTF Redfish, IPMI), uključujući podršku za Virtual Media i automatizovanu instalaciju i konfiguraciju servera, bez obavezne upotrebe vlasničkih alata pojedinačnih proizvođača.

2.2. Sloj kontejnerizacije i Kubernetes platforme (CaaS/PaaS)

Naša namjera je koristiti standardne Kubernetes distribucije, zasnovane na upstream Kubernetes tehnologiji i otvorenim standardima, koje moraju podržati napredne telco-specifične funkcionalnosti, uz osiguranu dugoročnu podršku i jasan, ažuran plan upravljanja životnim ciklusom (Lifecycle Management).

- **Certifikacija i distribucija:** Opisati podržane i preporučene verzije Kubernetes platforme, uključujući CNCF Kubernetes Conformance status za konkretne verzije, te navesti podržane distribucije i platforme (npr. Red Hat OpenShift, RKE2, Tanzu Kubernetes ili druga odgovarajuća rješenja). Navesti politiku podrške verzija (N-2), trajanje podrške i uobičajeni tok nadogradnje (upgrade) softverskih verzija platforme, uključujući međuzavisnosti i kompatibilnost sa zahtjevima koje postavljaju CNF aplikacije.
- **Napredni mrežni dodaci (CNI):** Opisati podržane mrežne dodatke (CNI) i mrežne komponente koje platforma omogućava, uključujući podršku za Calico, Cilium i Multus, te navesti zahtjeve koje pojedina CNF aplikacija postavlja prema primarnom CNI-ju i dodatnim mrežnim interfejsima.
- **Propusnost i niska latencija:** Opisati podršku za tehnologije poput SR-IOV (Single Root I/O Virtualization) i DPDK (Data Plane Development Kit), uključujući potrebnu konfiguraciju na nivou Kubernetes klastera, operativnog sistema, mrežnih kartica i pripadajuće mrežne opreme, kao i način dodjele i upravljanja hardverskim resursima.

- **Sigurnosni kontekst (Privileged Status):** Navesti konfiguracijske specifičnosti koje CNF kontejneri zahtijevaju za rad, uključujući potrebu za povlaštenim statusom (privileged: true), dodatnim Linux capabilities ili mogućnost rada unutar standardnih, restriktivnih sigurnosnih pravila (Pod Security Admission – PSA). Opisati mogućnosti platforme za kontrolu i upravljanje sigurnosnim politikama na nivou klastera, namespace-a i podova
- **Usklađenost platforme:** Platforma mora biti CNCF-conformant Kubernetes distribucija, uz podršku za aktuelne upstream verzije koje su u aktivnom ciklusu podrške, odnosno odgovarajuću politiku podrške verzija (N-2). Potrebno je opisati podršku za OCI-kompatibilne kontejnerske slike, Helm 4 (uključujući kompatibilnost i migraciju postojećih Helm 3 chartova), rad s više values datoteka, tpl templating i set-file opcije, kao i Operator obrazac i CRD-ove za upravljanje životnim ciklusom CNF-ova. Opisati mehanizam za upravljanje životnim ciklusom operatora (ugrađen u platformu ili zasnovan na otvorenim alatima, npr. Operator Lifecycle Manager, Helm ili GitOps) te, ukoliko postoji, katalog certificiranih ili validiranih operatora.
- **Operativni sistem node-ova:** Opisati operativni sistem koji se koristi na kontrolnim i radnim čvorovima. Poželjan je nepromjenjivi (immutable), za kontejnere optimizovan operativni sistem, kojim se upravlja i koji se nadograđuje kao sastavni dio platforme (jedinstven tok nadogradnje i model podrške). Prihvatljiv je i standardni enterprise Linux operativni sistem podržan od strane proizvođača platforme ili njegovog partnera, uz dostavljanje referentne dokumentacije i opisa načina nadogradnje, hardeninga i modela podrške.
- **Raspoređivanje i skaliranje:** Opisati podršku za Kubernetes resurse i mehanizme raspoređivanja i skaliranja, uključujući Deployments, StatefulSets i DaemonSets, Guaranteed QoS, Horizontal Pod Autoscaler (HPA v2) sa custom i eksternim metrikama, Vertical Pod Autoscaler (VPA), PodDisruptionBudgets, PriorityClasses i Preemption, Pod Topology Spread Constraints, te node/pod affinity i anti-affinity pravila.
- **Upravljanje performansama node-ova:** Opisati kako se CPU Manager (static politika), Topology Manager (single-numa-node, best-effort), Huge Pages, NUMA-aware raspoređivanje i Real-Time kernel konfigurišu i održavaju deklarativno (npr. putem profila performansi, operatora ili IaC/GitOps konfiguracije), uz mogućnost automatizovanog upravljanja kroz nadogradnje platforme i podršku proizvođača.
- **Visoko dostupan control plane:** Opisati referentnu arhitekturu visoke dostupnosti control plane-a, uključujući najmanje tri etcd člana i tri API server instance, njihov raspored na redundantnim kontrolnim čvorovima odvojenim od CNF radnih opterećenja, nadzor zdravlja etcd-a, mehanizme automatske kompakcije i defragmentacije, kao i enkripciju podataka u mirovanju (Encryption at Rest). Navesti način zaštite i oporavka etcd baze u slučaju otkaza.
- **Povišene Linux capabilities:** Opisati kako platforma, uz kontrolu putem sigurnosnih politika, omogućava rad opterećenja koja zahtijevaju dodatne Linux capabilities (npr. NET_RAW, NET_ADMIN ili SYS_ADMIN), bez automatske dodjele punog povlaštenog statusa (privileged: true). Navesti potrebna RBAC ovlaštenja za instalaciju i upravljanje Helm paketima, operatorima i pripadajućim CRD-ovima, uz primjenu principa najmanjih potrebnih privilegija (Least Privilege), bez nepotrebne dodjele cluster-admin ovlaštenja.

- **Integrisane platformske usluge:** Navesti koje su usluge uključene u isporuku platforme i pokrivene istim modelom podrške proizvođača, a koje zahtijevaju integraciju komponenti trećih strana. Obuhvatiti registar kontejnerskih slika sa skeniranjem ranjivosti, nadzor (monitoring), logovanje, GitOps, CI/CD, service mesh, upravljanje certifikatima, centralno upravljanje više klastera i napredne sigurnosne funkcionalnosti.
- **Messaging i data pipeline:** Opisati podršku za instalaciju i stabilan rad Apache Kafka klastera (pohrana i mreža), kao i ostalih stateful komponenti koje CNF-ovi koriste.

2.3. Mrežna infrastruktura, sinhronizacija i topologija

- **Fizički mrežni kapacitet:** Navesti preporučeni kapacitet fizičkih mrežnih interfejsa (npr. 2x25Gbps, 2x100Gbps) hardverski i aplikacijski potreban za podršku maksimalnom kapacitetu obrade saobraćaja. Navesti mogućnosti skaliranja mrežnog kapaciteta i redundantne povezivosti.
- **Granična latencija (RTT):** Navesti zahtjeve za mrežnom latencijom predloženog rješenja, uključujući maksimalne i preporučene vrijednosti RTT-a između čvorova, klastera i udaljenih lokacija, gdje je primjenjivo.
- **Vremenska sinhronizacija:** Postoje li zahtjevi za preciznu vremensku sinhronizaciju na razini hardvera (npr. PTP - Precision Time Protocol / IEEE 1588v2) ili je dovoljan standardni mrežni NTP. Navesti preciznost sinhronizacije koju aplikacije zahtijevaju.
- **Edge minimalna konfiguracija:** Navesti zahtjeve rješenja u pogledu udaljenih Edge lokacija i potrebe za implementacijom manjih Kubernetes klastera (npr. jedan fizički čvor ili kompaktni klaster od tri čvora), uključujući minimalne hardverske resurse, funkcionalna ograničenja i mogućnosti lokalnog rada u slučaju prekida veze prema centralnoj lokaciji.

- **Primarna i sekundarne mreže:** Opisati podršku za produkcijski CNI dodatak, kompatibilan sa Kubernetes standardima i podržan od proizvođača platforme (npr. OVN-Kubernetes, Calico, Cilium ili funkcionalno ekvivalentno rješenje), Multus ili ekvivalentan mehanizam za dodjelu više mrežnih interfejsa po podu, NetworkPolicy (ingress i egress) na nivou poda i namespace-a, IPv4/IPv6 dual-stack, SCTP protokol, te DSCP označavanje i očuvanje oznaka izlaznog saobraćaja radi integracije sa QoS politikama IP/MPLS transportne mreže. Navesti eventualna funkcionalna i tehnička ograničenja.
- **Eksterni pristup servisima:** Opisati podršku za LoadBalancer servise u bare-metal okruženju (L2 i BGP način rada), Ingress i Gateway API, kontrolisane izlazne (egress) IP adrese po namespace-u te integraciju sa eksternim DNS-om i load balancerima.
- **Upravljanje SR-IOV i DPDK resursima:** Opisati način na koji platforma deklarativno, putem odgovarajućih operatora i konfiguracijskih mehanizama, upravlja SR-IOV virtuelnim funkcijama (VF), DPDK user-space drajverima i mrežnim postavkama čvorova, uključujući listu podržanih mrežnih kartica (NIC) različitih proizvođača hardvera.
- **PTP uloge:** Ukoliko rješenje zahtijeva ili podržava PTP (prvenstveno za RAN i Edge opterećenja), navesti podržane PTP uloge (npr. T-GM, T-BC i OC, gdje je primjenjivo i uz odgovarajući hardver), podržane profile (npr. ITU-T G.8275.1), zahtjeve za hardverskim timestampingom i kompatibilnim mrežnim karticama, te način na koji se PTP konfiguriše, nadzire i alarmira kroz platformu.

- **Service mesh i mTLS:** Opisati podršku za Service Mesh, TLS i mTLS komunikaciju između CNF aplikacija i njihovih mikroservisa, uključujući mogućnosti integracije sa eksternim PKI sistemima, upravljanja certifikatima i definisanja sigurnosnih politika komunikacije. Navesti eventualna ograničenja primjene Service Mesh tehnologije na CNF data-plane saobraćaj.
- **Edge topologije i centralno upravljanje:** Navesti podržane topologije klastera (klaster sa jednim čvorom, kompaktni klaster od tri čvora, udaljeni radni čvorovi i standardni klaster sa više čvorova), uz opis funkcionalnih ograničenja i mogućnosti visoke dostupnosti za svaku topologiju. Opisati mogućnosti centralnog uvođenja, konfiguracije, nadogradnje i održavanja udaljenih lokacija bez potrebe za izlaskom na teren (Zero-Touch Provisioning), uključujući primjenu GitOps pristupa.

2.4. Pohrana podataka i upravljanje stanjem

- **Klase pohrane i CSI:** Kakvu vrstu pohrane podataka (Storage) zahtijeva vaša arhitektura i podržava li standardni CSI (Container Storage Interface)?
- **Performanse pohrane (IOPS):** Za predloženo tehničko rješenje navesti detaljan opis podržanih performansi pohrane, uključujući IOPS, propusni opseg (throughput) i latenciju, u odnosu na zahtjeve sistema.
- **Stateless Arhitektura:** Jesu li ključne mrežne funkcije potpuno stateless ili zahtijevaju perzistentnu pohranu podataka i očuvanje stanja?
- **Funkcionalnosti pohrane:** Navesti podržane funkcionalnosti PersistentVolumes (PV) i dinamičkog provisioninga, block, file i object storage tipove, proširenje volumena (poželjno online), CSI VolumeSnapshot i kloniranje volumena, te mogućnosti QoS izolacije kojima se osigurava da opterećenje jednog CNF-a ne utiče na performanse pohrane drugih CNF-ova koji koriste zajedničku infrastrukturu.

- **Softverski definisana pohrana:** Navesti da li proizvođač platforme nudi integrisano softverski definisano rješenje za pohranu podataka u okviru iste platforme, kao i listu certificiranih CSI drajvera za integraciju s eksternim storage sistemima.
- **Backup, restore i replikacija:** Opisati podršku za backup i restore aplikacija, uključujući Kubernetes objekte i perzistentne volumene, replikaciju podataka između zona/lokacija, kao i podržane scenarije oporavka od katastrofe (Disaster Recovery – DR).

2.5. Sigurnost i hardening platforme

Platforma treba biti isporučena u ojačanom (hardened) stanju. Detaljni zahtjevi dati su u Prilogu 1, a u nastavku se traži opis ključnih sigurnosnih mehanizama.

- **Hardening i usklađenost:**Opisati usklađenost sa CIS Kubernetes Benchmarkom (ili CIS benchmarkom za konkretnu distribuciju) i CIS benchmarkom operativnog sistema čvorova, sa NIST SP 800-190 i NIST SP 800-204, te alate kojima se usklađenost automatski provjerava, ocjenjuje i otklanjaju utvrđena odstupanja (npr. kube-bench, OpenSCAP, Compliance Operator). Navesti verzije primijenjenih benchmarka, ostvareni nivo usklađenosti, način periodične provjere i posjedovane certifikate (npr. FIPS 140, Common Criteria), uz navođenje konkretnog nivoa certifikacije i pripadajućih certifikata.

- **Sigurnost poda i mandatory access control:** Opisati primjenu Pod Security Standards (Baseline/Restricted kao zadano), dodatne mehanizme ograničavanja privilegija koje platforma nudi iznad standardnog PSA, rad kontejnera bez root privilegija, Seccomp profile te SELinux ili AppArmor. Preporučuje se da mandatory access control (SELinux, AppArmor ili ekvivalent) bude uključen i u enforcing načinu rada po zadanim postavkama.
- **Identitet i pristup:** Opisati RBAC model (namespace i cluster nivo), princip najmanjih privilegija, integraciju sa eksternim IdP sistemima (OIDC, LDAP) i evidenciju svih povlaštenih operacija, uključujući mogućnosti centralizovanog upravljanja korisnicima, grupama i privilegijama.
- **Secrets i enkripcija:** Opisati enkripciju etcd-a u mirovanju, integraciju sa eksternim KMS-om i sistemima za upravljanje tajnama (npr. HashiCorp Vault, CyberArk, External Secrets Operator) te automatizovano upravljanje certifikatima (cert-manager, ACME, eksterni PKI).
- **Sigurnost lanca isporuke:** Opisati provjeru potpisa kontejnerskih slika pri prijemu (Cosign / Notary v2), integrisano skeniranje ranjivosti u registru, politike kao kod (OPA Gatekeeper, Kyverno ili ekvivalent), te način na koji proizvođač potpisuje i objavljuje vlastite slike, sigurnosne zakrpe i CVE obavijesti. Navesti da li platforma omogućava automatsko blokiranje neprovjerenih, nepotpisanih ili ranjivih slika na osnovu definisanih sigurnosnih politika.
- **Mrežna izolacija i audit:** Opisati zadanu deny-all NetworkPolicy politiku za nove namespace-ove, ograničenje pristupa Kubernetes API-ju isključivo sa management mreža, API audit logovanje i prosljeđivanje logova u eksterni SIEM. Navesti da li se mrežna izolacija i primjena NetworkPolicy politika podržavaju nativno ili putem dodatnog CNI rješenja, kao i način implementacije i upravljanja ovim politikama.
- **Sigurnost u radu (runtime):** Navesti da li platforma uključuje alate za otkrivanje prijetnji u radu, upravljanje ranjivostima i provjeru usklađenosti na nivou više klastera.

2.6. Upravljanje životnim ciklusom, automatizacija i rad sa više klastera

- **Automatizovana instalacija:** Opisati potpuno automatizovanu i ponovljivu instalaciju klastera iz koda (Infrastructure-as-Code), uključujući podršku za alate kao što su Terraform, Ansible ili ekvivalent, te instalaciju u izolovanom (air-gapped) okruženju, sa svim artefaktima dostupnim offline (slike, Helm paketi, operatori, OS paketi). Navesti mogućnosti automatizacije konfiguracije i inicijalnog podešavanja klastera nakon instalacije.
- **Nadogradnje bez prekida:** Opisati rolling nadogradnju control plane-a i radnih čvorova bez prekida rada klastera, uz poštivanje PodDisruptionBudgets (drain → upgrade → rejoin), kanarinske nadogradnje dijela čvorova prije cijele flote, blue/green nadogradnje klastera te automatizovano sigurnosno ažuriranje operativnog sistema sa mogućnošću povrata (rollback). Navesti očekivani uticaj nadogradnji na dostupnost aplikacija i CNF-ova, kao i mogućnosti provjere kompatibilnosti prije nadogradnje. Moguće je opisati i drugačiji podržani model nadogradnje pored prethodno navedenih.
- **Dugoročna podrška verzija:** Navesti trajanje podrške po verziji i postojanje verzija sa produženom podrškom. Opisati postupak nadogradnje između takvih verzija i njegov uticaj na radne čvorove (npr. broj potrebnih ciklusa restarta i očekivano trajanje), te dostupnost

kritičnih ispravki bez prelaska na novu minor verziju. Navesti politiku objavljivanja sigurnosnih zakrpa, rokove podrške i postupanje u slučaju otkrivanja kritičnih ranjivosti.

- **GitOps i self-healing:** Opisati ugrađenu ili podržanu GitOps podršku (preporuka ili slično: Argo CD, Flux, Fleet), otkrivanje i ispravljanje odstupanja konfiguracije (CRD, Helm release), te self-healing platforme – automatsko otkrivanje i zamjenu neispravnog čvora.
- **Upravljanje više klastera:** Opisati centralno upravljanje životnim ciklusom, politikama, usklađenošću i nadzorom većeg broja klastera (core, regionalne i edge lokacije) iz jedne tačke, uključujući zero-touch uvođenje novih klastera. Navesti da li centralno upravljanje omogućava jedinstven pregled stanja svih klastera, centralizovano upravljanje konfiguracijama i politikama, kao i delegiranje administrativnih privilegija po klasterima ili lokacijama.
- **Multi-tenancy i uvođenje CNF-ova:** Opisati multi-tenancy zasnovan na namespace-ovima (kvote, LimitRange), samouslužno kreiranje namespace-ova putem GitOps tokova i dostupnost validiranog vodiča za uvođenje (onboarding) CNF-ova koji pokriva RBAC, NetworkPolicy, StorageClass i admission politike.
- **CI/CD integracija:** Opisati integraciju sa CI/CD sistemima (npr. GitLab), registrima kontejnerskih slika te podršku za blue/green i canary isporuku aplikacija.

2.7. Visoka raspoloživost, kontinuitet poslovanja i oporavak od katastrofe (HA, BC/DR)

S obzirom na namjenu platforme (kritični telekomunikacijski servisi), od učesnika se traži opis ponašanja rješenja i preporučenih mjera u sljedećim scenarijima:

- **Otkaz čvorova i lokacije:** Opisati ponašanje platforme i CNF-ova pri otkazu jednog čvora, više čvorova ili cijele lokacije, uključujući očekivano vrijeme oporavka i uticaj na saobraćaj.
- **Redundantnost control plane-a:** Opisati mehanizme redundantnosti control plane-a i ponašanje klastera pri gubitku kvoruma etcd-a.
- **Domene otkaza:** Opisati anti-affinity pravila i raspoređivanje opterećenja preko domena otkaza (čvor, rack, zona, lokacija).
- **Gubitak mreže ili pohrane:** Opisati ponašanje platforme i CNF-ova pri gubitku mrežne povezanosti ili nedostupnosti storage-a (npr. split-brain scenariji i ponovno uspostavljanje veze).
- **Rezervni kapacitet:** Opisati preporučeni rezervni kapacitet i N+1 (ili N+M) dizajn za control plane, radne čvorove i pohranu.
- **RTO i RPO:** Navesti ostvarive RTO (Recovery Time Objective) i RPO (Recovery Point Objective) vrijednosti za platformu i odgovarajuće servise, te preduslove za njihovo postizanje. Navesti da li su navedene vrijednosti garantovane, projektovane ili ostvarene kroz testiranja, uz navođenje rezultata relevantnih testova.
- **Testiranje DR scenarija:** Opisati procedure i alate za periodično testiranje disaster recovery scenarija, uključujući preporučenu učestalost i način dokumentovanja rezultata.
- **HA i DR za CNF okruženje:** Opisati podršku platforme za visoku raspoloživost i DR funkcionalnosti CNF-ova (geo-redundantni klasteri, replikacija stanja, prebacivanje saobraćaja između lokacija).

2.8. Hardver i mrežna oprema – ponuda dobavljača

Ovo poglavlje namijenjeno je prikupljanju informacija o serverskoj i mrežnoj opremi koja može činiti osnovu buduće Telco Cloud infrastrukture. Može poslužiti kao smjernica za definisanje sveobuhvatnog infrastrukturnog rješenja u okviru ponude kontejnerske platforme, ali i kao osnova za zasebnu ponudu hardverske infrastrukture koju bi BH Telecom nabavljao i stavljao na raspolaganje za implementaciju različitih kontejnerskih platformi i CNF rješenja (Customer-Owned Infrastructure, based on an approved/validated BOM).

Cilj je osigurati da ponuđena oprema bude validirana i službeno podržana sa različitim kontejnerskim platformama i CNF rješenjima, bez vezivanja za jednog proizvođača.

Molimo dobavljače da opišu:

- **Mrežna oprema (ToR, leaf/spine):** Opisati ponuđenu mrežnu opremu i preporučenu arhitekturu (leaf-spine ili ekvivalent): broj i brzine portova (npr. 25/100/400 Gbps), podršku za EVPN-VXLAN, BGP (uključujući BGP peering sa LoadBalancer servisima klastera), multihoming (MC-LAG, ESI ili ekvivalent), ECMP, QoS/DSCP, jumbo frame-ove te operativni sistem mrežne opreme i mogućnost korištenja otvorenih mrežnih operativnih sistema.
- **Sinhronizacija na mrežnoj opremi:** Ukoliko je primjenjivo (RAN i edge opterećenja), navesti podršku mrežne opreme i mrežnih kartica za PTP (IEEE 1588v2, ITU-T G.8275.1; uloge T-BC i T-TC) i SyncE, te zahtjeve prema izvoru vremena.
- **Automatizacija i upravljanje mrežom:** Opisati programske interfejse mrežne opreme (NETCONF/YANG, gNMI, REST API), integraciju sa alatima za automatizaciju (npr. Ansible, Terraform) i GitOps tokovima, zero-touch provisioning switcheva te streaming telemetriju prema otvorenim sistemima za nadzor.
- **Serverske platforme:** Navesti ponuđene modele servera i njihove ključne karakteristike: procesore, memoriju, lokalnu pohranu, mrežne kartice (podrška za SR-IOV i DPDK), SmartNIC/DPU i GPU akceleratore, TPM 2.0 i Secure Boot, redundantno napajanje te potrošnju energije i energetsku efikasnost po profile. Navesti podršku za NUMA arhitekturu, mogućnosti BIOS optimizacije za mrežna i telco opterećenja te preporučene konfiguracije za rad sa DPDK i SR-IOV tehnologijama.
- **Firmver i BIOS:** Opisati upravljanje životnim ciklusom firmvera (BIOS/UEFI, BMC, mrežne kartice, storage kontroleri): alate za centralizovano i automatizovano ažuriranje (npr. putem Redfish-a), učestalost izdavanja, objavljivanje sigurnosnih zakrpa i CVE obavijesti, potpisivanje firmvera, mogućnost povrata na prethodnu verziju te usklađenost verzija firmvera i drajvera s podržanim verzijama kontejnerske platforme.
- **Validacija s kontejnerskim platformama:** Navesti Kubernetes/CaaS distribucije i njihove verzije s kojima je ponuđeni hardver certificiran ili validiran (uključujući drajvere i operatore za mrežne kartice i akceleratore), postojeće zajedničke referentne arhitekture s proizvođačima platformi, te da li je hardver uvršten u javno dostupne liste certificiranog hardvera tih proizvođača. Navesti konkretne validirane kombinacije verzija hardvera, firmwarea, drajvera i kontejnerske platforme, kao i način održavanja njihove međusobne kompatibilnosti tokom životnog ciklusa.

- **Validacija sa CNF-ovima:** Navesti da li je ponuđena oprema validirana u referentnim konfiguracijama proizvođača telco aplikacija (5G Core, IMS, signalizacija, RAN i dr.), uz navođenje proizvođača i referenci iz produkcijskih okruženja.
- **Podrška:** Opisati model podrške za hardver i mrežnu opremu: dostupnost 24x7, vremena odziva i otklanjanja kvara po nivoima ozbiljnosti, prisustvo servisa i inženjera u Bosni i Hercegovini, lokalno skladište rezervnih dijelova, rokove zamjene dijelova (npr. 4 sata ili sljedeći radni dan), podršku na lokaciji, mogućnost zadržavanja neispravnih diskova te proces eskalacije i saradnje sa proizvođačem platforme i proizvođačima CNF-ova pri rješavanju incidenata.
- **Garancija i životni ciklus opreme:** Navesti trajanje standardne garancije i mogućnost produženja (npr. na 3, 5 ili 7 godina), planirane datume prestanka prodaje i podrške (EoS/EoL) za ponuđene modele, minimalni period podrške i dostupnosti rezervnih dijelova nakon prestanka prodaje, te politiku najave promjena životnog ciklusa.
- **Hardverska sigurnost i lanac isporuke:** Opisati mehanizme hardverskog korijena povjerenja (root of trust), provjere integriteta firmvera pri pokretanju, zaštite BMC interfejsa, te način na koji se osigurava i dokazuje integritet opreme kroz lanac isporuke.

Virtuelizacija kao opcionalna varijanta platforme:

Učesnici koji uz kontejnersku platformu nude i podršku za izvršavanje virtuelnih mašina na istoj platformi (produkcijski dokazan hipervizor, zajedničko upravljanje, mreža i pohrana, live migracija, backup i alati za migraciju sa postojećih virtuelizacijskih platformi) mogu te informacije dostaviti u slobodnoj formi u okviru svojih odgovora. Dostavljanje ovih informacija nije obavezno i neće biti uslov za ocjenu usklađenosti sa zahtjevima za kontejnersku platformu. Ipak, smatrat će se dodatnom vrijednošću, jer BH Telecomu omogućava da procijeni mogućnost konvergencije kontejnera i virtuelnih mašina na jednoj platformi. Uslovi i zahtjevi za virtuelizacijsku platformu mogu se dodatno uskladiti kroz interaktivnu komunikaciju između BH Telecoma i partnera/vendora. Sve nejasnoće i upite molimo da uputite putem standardnih kanala komunikacije.

3. MATRICA TEHNIČKIH PREDUSLOVA

3.1. Matrica – Telco Cloud referentna arhitektura (kontejnerska platforma)

Narednom tabelom definisani su tehnički parametri za opis i poređenje ponuđenih Telco Cloud rješenja (kontejnerskih platformi). Dobavljači su dužni za svaki navedeni tehnički parametar popuniti kolonu „Preporučeni infrastrukturni / softverski zahtjev“ podacima koji odgovaraju ponuđenom rješenju, uključujući podržane funkcionalnosti, tehnologije, kapacitete i konfiguracije. U koloni „Napomena / Komentar“ navesti eventualna ograničenja, specifičnosti, odstupanja i dodatna pojašnjenja, uz dostavljanje relevantne tehničke dokumentacije gdje je primjenjivo.

Tehnički parametar	**Preporučeni infrastrukturni / softverski zahtjev**	**Napomena / Komentar dobavljača (opreme ili softvera)**
K8s verzije		
Podržana CPU arhitektura (x86 / ARM)		
Max broj vCPU dodijeljen jednom podu		
Max memorija u MB dodijeljena jednom podu		
Max kapacitet diska u GB dodijeljen jednom podu		
Max broj mrežnih konekcija dodijeljen jednom podu		
SR-IOV / DPDK / PCI Passthrough		
SmartNICs		
Hardware coprocessor support (GPU/NPU)		
Storage Block		
CPU allocation ratio		
CPU Pinning		
NUMA		
HugePages		
Podrška VXLAN, MPLSoUDP, GENEVE, i sl.		

Zahtjevi za Storage (IOPS / CSI)		
Zahtjevi za CNI		
PTP vremenska sinhronizacija		
Model instalacije		
Operativni sistem čvorova		
Control plane		
Topologije klastera		
Eksterni pristup (LoadBalancer / Ingress)		
Sigurnosni hardening		
Nadogradnje platforme		
Upravljanje više klastera i GitOps		
Observability		
Otvorenost koda		
Podrška i životni ciklus		
Model licenciranja		
Visoka raspoloživost i DR		
Onboarding i upgrade CNF-ova		
Indikativne cijene i licence		
Dodatni parametri	Navedite sve dodatne parametre i specifičnosti koje smatrate da je potrebno uzeti u obzir, a nisu prevashodno navedeni u ovoj tabeli.	

Vrijednosti i karakteristike koje dobavljači navedu u koloni „Preporučeni infrastrukturni / softverski zahtjev“ predstavljaju opis ponuđenog rješenja i osnovu za tehničko poređenje. Dobavljači su dužni navesti podržane vrijednosti, funkcionalnosti i eventualna ograničenja, uz odgovarajuće obrazloženje. Isto se odnosi i na zahtjeve iz Priloga 1, uključujući one formulisane kao „mora“ ili „ne smije“, koji izražavaju ciljno stanje platforme. Eventualna odstupanja potrebno je jasno navesti i obrazložiti.

3.2. Detaljna izjava o usklađenosti (SoC)

Detaljni zahtjevi za telco-grade Kubernetes platformu dati su u Prilogu 1 ovog dokumenta, u formi izjave o usklađenosti (Statement of Compliance). Molimo dobavljače kontejnerske platforme da za svaki zahtjev navedu stepen usklađenosti (potpuno usklađeno, djelimično usklađeno, nije usklađeno ili nije primjenjivo), uz odgovarajuće obrazloženje, opis načina implementacije i eventualnih ograničenja. Gdje je primjenjivo, potrebno je navesti i referentnu tehničku dokumentaciju.

U slučaju potrebe i složenosti ponude moguće je dodatno dopuniti tabelu prema vlastitom nahođenju i u skladu s RFI obimom.

4. USLOVI ZA POTPUNU PODRŽANOST I RAZGRANIČENJE ODGOVORNOSTI U MULTI-VENDOR OKRUŽENJU

Kako bismo osigurali da naša zajednička infrastruktura bude u potpunosti podržana i da izbjegnemo "siva područja" odgovornosti prilikom operacija u multi-vendor okruženju, molimo vas da odgovorite na sljedeća strateška pitanja:

4.1. Certifikacija i usklađenost s otvorenim standardima

- **Kubernetes kompatibilnost:** Podržavate li (kao ponuđač softvera) odnosno možete li isporučiti (kao dobavljač opreme) rješenja kompatibilna sa Kubernetes distribucijama koje posjeduju važeći CNCF Certified Kubernetes Conformance certifikat? Navesti podržane distribucije i verzije, kao i eventualna ograničenja ili zavisnosti od specifičnih proizvođačkih komponenti.
- **GSMA Anuket usklađenost:** Navesti da li je predloženo rješenje usklađeno sa GSMA Anuket preporukama i referentnim arhitekturama za cloud-native telekomunikacijsku infrastrukturu, uključujući GSMA NG.139, gdje je primjenjivo. Ukoliko rješenje nije usklađeno, navesti alternativne preporuke i standarde na kojima se zasniva, uz opis načina na koji se osiguravaju interoperabilnost i podrška za multi-vendor okruženja. Dostaviti referentnu listu implementiranih multi-vendor okruženja u regionu i svijetu.
- **Open source:** Da li je kontejnerska platforma u cijelosti (100%) otvorenog koda ili se oslanja na open-core / vlasničke komponente? (Ovo nije eliminatoran zahtjev, ali je jedna od preporuka.) Navesti upstream projekte na kojima se zasniva i licence pod kojima su objavljeni, te za eventualne vlasničke komponente opisati kako se osigurava prenosivost opterećenja i izlazak sa platforme (exit strategija). Ako platforma nije open-

source, dostaviti referentne dokumente koji opisuju rješenje i dokaz su pouzdanosti rješenja (pouzdana produkcijska upotreba).

- **Doprinos zajednici (community):** Opisati ulogu proizvođača (ili njegovih partnera čije komponente rješenje koristi) u upstream zajednicama (Kubernetes i srodni CNCF projekti): obim doprinosa kodu, eventualno učešće ili vođenje SIG grupa i uticaj na smjer razvoja tehnologije. Odgovor ima informativni karakter i nije uslov za ocjenu usklađenosti.
- **Standardi:** Navesti usklađenost sa ETSI GS NFV-IFA 011 i ETSI GS NFV-SOL 001/002 (gdje je primjenjivo), 3GPP TS 28.530 / TS 28.531 (izolacija mrežnih slice-ova na nivou platforme), GSMA NG.139, preporukama CNCF telekom zajednice te NIST SP 800-190 i SP 800-204. Za svaki navedeni standard potrebno je opisati njegovu primjenjivost na predloženo rješenje i navesti odgovarajuće dokaze o usklađenosti ili podršci.
- **Certifikacija CNF-ova:** Da li proizvođač platforme ima program certifikacije/validacije telco aplikacija (CNF) ili ekvivalentan dokaz interoperabilnosti (zajednička validacija sa proizvođačima CNF-ova, otvoreni alati poput Anuket CNF Test Suite i Anuket referentnih testova, odnosno drugi ekvivalentni alati za provjeru interoperabilnosti i usklađenosti CNF-ova), te javno dostupan alat za provjeru usklađenosti CNF-ova sa najboljim praksama? Navesti listu certificiranih ili validiranih CNF-ova i proizvođača (5G Core, signalizacija, IMS, RAN i dr.), uz navođenje testirane verzije platforme.
- **Validirana telco referentna konfiguracija:** Da li proizvođač za svaku verziju platforme objavljuje validiranu i testiranu referentnu konfiguraciju za telco core i RAN opterećenja?
- **Portabilnost:** Potvrditi mogućnost prenosivosti kontejnerskih opterećenja između različitih Kubernetes platformi bez potrebe za izmjenama i ponovnom izgradnjom kontejnerskih slika, uz navođenje eventualnih ograničenja i zavisnosti od specifičnih infrastrukturnih ili proizvođačkih komponenti. Navesti infrastrukturna okruženja na kojima se ista platforma može koristiti (bare-metal, virtuelizovana infrastruktura, javni cloud) uz jednako ili uporedivo operativno iskustvo; podrška za javni cloud smatra se dodatnom vrijednošću.

4.2. Razgraničenje odgovornosti i validacija

- **Infrastrukturni KPI-jevi:** Navesti mjerne parametre (npr. mrežna latencija unutar klastera, gubitak paketa, jitter, propusni opseg) i njihove garantovane granične vrijednosti koje infrastruktura mora ispunjavati kako bi proizvođač mogao preuzeti punu odgovornost za podršku i rad platforme. Navesti način mjerenja, uslove testiranja i eventualne zavisnosti od hardverske i mrežne konfiguracije.
- **Alati za provjeru spremnosti:** Nudite li automatizovane skripte ili alate za provjeru spremnosti infrastrukture (Readiness Check Tools / Pre-flight Checks) koje je moguće pokrenuti prije instalacije platforme? Navesti koje parametre provjeravaju i da li generišu izvještaj o ispunjenosti preduslova za instalaciju.
- **Ograničenja platforme:** Postoje li specifične hardverske komponente, mrežni (CNI) ili skladišni (CSI) dodaci, kao i druge infrastrukturne komponente ili konfiguracije

koje vaše rješenje izričito ne podržava? Navesti poznata ograničenja i listu podržanih alternativa.

- **Jedna tačka podrške:** Da li jedan proizvođač, odnosno jedan ugovorni partner uz odgovarajuće back-to-back ugovore o podršci, preuzima koordinaciju i odgovornost za podršku operativnom sistemu čvorova, Kubernetes platformi i svim pripadajućim platformskim uslugama? Ako je model podrške drugačiji, detaljno ga opisati, uključujući jasno razgraničenje odgovornosti između uključenih proizvođača. Opisati model saradnje sa proizvođačima CNF-ova i hardvera pri rješavanju incidenata, uključujući zajedničke procese podrške, eskalacije i upravljanje incidentima.
- **Certificirani hardver:** Navesti javno dostupnu listu certificiranog ili validiranog hardvera (serveri, mrežne kartice, akceleratori) različitih proizvođača, uz navođenje podržanih modela, verzija firmware-a i eventualnih ograničenja kompatibilnosti.
- **Isporuke dobavljača platforme:** Dostaviti referentnu arhitekturu, listu podržanih verzija, validirane mrežne i storage konfiguracije, vodič za Day-2 operacije, kao i dokumentaciju za nadogradnju, održavanje i upravljanje životnim ciklusom platforme.

4.3. Multi-App Hosting & Isolation

Budući da je plan da naša platforma istovremeno pokreće kritične telekomunikacijske servise i druga relevantna napredna cloud-native rješenja, stabilnost i prevencija uticaja jednih na druge su nam apsolutni prioritet.

- **Izolacija resursa (Noisy Neighbor):** Koje mehanizme izolacije (npr. Kubernetes Namespaces, Resource Quotas, Cgroups) zahtijevate ili podržavate kako bi 5G core servisi imali zagarantovane resurse?
- **Visoka dostupnost (Anti-Affinity):** Sadrže li vaši instalacijski paketi / hardverske politike nativna pravila za raspoređivanje opterećenja i kontejnera na različite fizičke servere (Node Anti-Affinity)?
- **Izolacija po proizvođaču i funkciji:** Opisati primjenu zasebnih namespace-ova po proizvođaču CNF-a i po funkciji, ResourceQuota i LimitRange, Taints/Tolerations i PriorityClasses te mrežnu izolaciju između tenant-a.
- **Raspored po zonama i rack-ovima:** Opisati Pod Topology Spread Constraints i anti-affinity na nivou rack-a i zone za kritične CNF podove.

4.4. Ops & Observability

- Može li se vaše rješenje (hardverski telemetrijski alati ili softverski agenti) u potpunosti integrisati s otvorenim i standardnim sistemima za nadzor (npr. Prometheus, Grafana, OpenTelemetry, Graylog i sl.)?
- **Metrike:** Opisati izlaganje Prometheus-kompatibilnih metrika za sve komponente platforme (API server, etcd, kubelet, CNI, CSI), dugoročno čuvanje metrika, kontrolu kardinalnosti te custom metrics adapter za HPA v2.
- **Alarmi:** Opisati unaprijed pripremljena pravila alarmiranja za narušavanje SLO-a platforme (nedostupnost čvora, OOMKill, etcd latencija, popunjenost PVC-a),

Alertmanager (rutiranje, grupisanje, potiskivanje), prosljeđivanje alarma u NOC alate putem webhook-a i otkrivanje anomalija.

- **Logovi:** Opisati platformski upravljanu agregaciju logova, strukturirano (JSON) logovanje, prosljeđivanje u eksterni SIEM (syslog, Kafka, Elasticsearch-kompatibilan endpoint) i čuvanje logova najmanje 90 dana. Jasno navesti da li je navedeno čuvanje logova obuhvaćeno rješenjem ili zahtijeva dodatnu infrastrukturu, licence ili eksterne sisteme za pohranu.
- **Vizualizacija:** Opisati unaprijed pripremljene dashboard-e za stanje klastera, čvorova i opterećenja te jedinstven prikaz za više klastera.

4.5. Podrška, životni ciklus i suverenitet

- **Model podrške:** Opisati 24x7 podršku, nivoe ozbiljnosti i vremena odziva, prisustvo i jezik podrške u regionu/EU te direktan pristup inženjerima proizvođača za kritične sigurnosne ranjivosti.
- **Regulatorna usklađenost:** Opisati kako model podrške i obrade podataka ispunjava zahtjeve zaštite podataka (GDPR) i sigurnosti mrežnih i informacionih sistema (NIS2), gdje je primjenjivo. Navesti konkretne tehničke i organizacione mjere, mehanizme zaštite podataka, kontrolu pristupa, lokaciju obrade i pohrane podataka, kao i način osiguravanja kontrole nad podacima i nezavisnosti od jednog dobavljača.
- **Ispravke i dugoročna podrška:** Navesti da li se kritične ispravke isporučuju za postojeću verziju bez obavezne nadogradnje na novu, trajanje životnog ciklusa verzija i dokazanu praksu redovnog izdavanja enterprise verzija.
- **Stručne usluge i obuka:** Navesti dostupne stručne usluge (dizajn, implementacija, migracija, uvođenje CNF-ova), programe obuke i certifikacije te lokalne partnere.
- **Reference:** Navesti reference produkcijskih implementacija Telco Cloud platforme kod telekom operatora u regionu i svijetu, sa CNF-ovima više proizvođača.
- **Licenciranje:** Opisati model licenciranja (jedinica, uključene komponente, uslovi za bare-metal i edge lokacije) i šta je obuhvaćeno jednom pretplatom.

4.6. Onboarding, integracija i upravljanje životnim ciklusom CNF-ova u multi-vendor okruženju

Iskustva sa postojećim virtuelizacijskim (VNF) platformama pokazala su da značajan izazov predstavlja koordinacija između proizvođača platforme, proizvođača mrežnih funkcija i operatera. Stoga se od učesnika traži jasan opis modela onboardinga, integracije i lifecycle podrške za CNF-ove različitih proizvođača, uključujući definisanje odgovornosti eventualnog sistem integratora:

- **Onboarding i orkestracija:** Opisati podršku platforme za onboarding, lifecycle management i orkestraciju CNF-ova različitih telekom proizvođača, uključujući Kubernetes-native funkcionalnosti potrebne za njihov rad.
- **Odgovornosti:** Definisati odgovornosti za onboarding, validaciju i integraciju CNF-ova različitih proizvođača na platformu.
- **Model saradnje:** Opisati model saradnje između vlasnika platforme (BH Telecom), proizvođača platforme, proizvođača CNF-a i eventualnog sistem integratora.

- **Uloga sistem integratora:** Navesti da li je za onboarding i integraciju CNF-ova predviđena uloga sistem integratora, te koje aktivnosti i nadležnosti su obuhvaćene njegovim angažmanom.
- **Procedure onboardinga:** Navesti da li platforma podržava certificirane ili verificirane procedure za onboarding CNF-ova različitih proizvođača.
- **Granica CNF – platforma:** Definisati odgovornost za rješavanje problema koji nastaju na granici između CNF-a i platforme (fault isolation i troubleshooting u multi-vendor okruženju).
- **Automatsko skaliranje:** Opisati automatsko horizontalno i vertikalno skaliranje CNF-ova u skladu sa opterećenjem, uključujući korištene mehanizme, preduslove, ograničenja i podršku za stateful i stateless CNF-ove.
- **Nadzor CNF-ova:** Opisati automatizovano praćenje performansi, alarmiranje i troubleshooting CNF-ova.
- **Deployment, update i upgrade:** Opisati način izvršavanja deployment-a, redovnih update-a i upgrade-a platforme i CNF-ova (koji čine određenu mrežnu funkcionalnost), korištenje CI/CD pipeline-a, upravljanje kompatibilnošću verzija platforme i CNF-ova, postupke testiranja i validacije, planirane vremenske okvire za izvođenje upgrade-a i preporučenu učestalost nadogradnji.
- **ISSU CNF-ova:** Opisati mogućnosti i način izvođenja In-Service Software Upgrade (ISSU) – nadogradnje softvera CNF-a uz zadržavanje postojeće verzije Cloud platforme, pri čemu se osigurava kontinuitet obrade saobraćaja na CNF-u (zero-downtime ili minimal-downtime upgrade). Navesti preduslove, ograničenja i eventualni uticaj na aktivne sesije i korisnički saobraćaj.
- **Upgrade platforme:** Opisati mogućnosti i način izvođenja upgrade-a softvera Cloud platforme uz zadržavanje postojećih verzija CNF-ova, uključujući zahtjeve za kompatibilnošću, preduslove i eventualni uticaj na rad i dostupnost telekomunikacijskih servisa.
- **Rollback:** Opisati mogućnost povrata (rollback) na prethodnu verziju CNF-a u slučaju neuspješnog upgrade-a, uključujući postupak izvođenja, vremenski okvir i eventualna ograničenja.
- **Preduslovi i ograničenja:** Definisati sve preduslove koje je potrebno ispuniti na strani CNF-ova kako bi se osiguralo uspješno izvršenje update/upgrade-a. Navesti situacije u kojima je potreban redeployment CNF-a ili offline upgrade i koliko u tim slučajevima traje procedura, uzimajući u obzir zahtijevanu pouzdanost telco servisa i minimalan uticaj na korisnike.
- **Dostupnost, sigurnost i interoperabilnost:** Pojasniti na koji način ponuđač osigurava visok nivo dostupnosti, sigurnosti i interoperabilnosti CNF-ova različitih proizvođača sa Cloud platformom, uključujući mehanizme validacije, upravljanje kompatibilnošću verzija i rješavanje problema u multi-vendor okruženju.

4.7. Dokazi i prateća dokumentacija

Uz odgovore na RFI, molimo učesnike da, u mjeri u kojoj je to moguće, dostave sljedeće dokaze i prateću dokumentaciju:

- primjere implementacija u produkcijskim telekomunikacijskim okruženjima.

- reference uspješnih multi-vendor telco cloud implementacija u kojima se na istoj platformi izvršavaju CNF-ovi više proizvođača, uz navođenje proizvođača CNF-ova i sistema o kojima se radi;
- opis iskustva s multi-vendor integracijama;
- tehničke izvještaje o testiranju performansi;
- relevantne certifikate i njihove verzije;
- aktuelnu matricu kompatibilnosti (verzije platforme, hardvera i CNF-ova);
- primjer runbook-a ili postupka za dijagnostiku;
- primjer plana nadogradnje
- dokumentaciju o poznatim ograničenjima, zavisnostima i kompatibilnosti između platforme, hardvera i CNF-ova različitih proizvođača.

4.8. Komercijalne informacije i indikativne cijene

BH Telecom je svjestan da cijene variraju u vremenu i u zavisnosti od veličine projekta, te da u ovoj fazi nisu definisani kapaciteti ni konkretni CNF-ovi. Ipak, radi planiranja, molimo učesnike da, ukoliko je moguće, dostave indikativne jedinične cijene za:

- tipične serverske konfiguracije i ostalu opremu;
- Kubernetes/CaaS platformu;
- dodatne licence i pretplate;
- instalaciju i integraciju;
- podršku i održavanje;
- nadogradnje i migracije;
- rezervni kapacitet i disaster recovery;
- obuku i prenos znanja.

Molimo da indikativne cijene serverske opreme budu iskazane za 2–3 referentna profila (npr. control plane, opšti radni čvor, high-performance radni čvor sa SR-IOV/DPDK) prema vlastitoj preporuci, uz tehničku specifikaciju svakog profila.

Radi uporedivosti odgovora, molimo da indikativne cijene budu iskazane u skladu sa sljedećim:

- **Valuta i datum:** cijene iskazati u EUR i BAM, bez PDV-a, uz navođenje datuma na koji se cijene odnose i okvirnog perioda njihove važnosti.
- **CAPEX / OPEX:** odvojeno iskazati jednokratne troškove (oprema, trajne licence, instalacija i integracija) i ponavljajuće godišnje troškove (pretplate, podrška i održavanje).
- **TCO:** dostaviti okvirni ukupni trošak vlasništva (TCO) za period od 3 i 5 godina, uz jasno navedene pretpostavke (broj i profil čvorova, broj klastera i lokacija, nivo podrške).
- **Obrazac:** cijene, gdje je moguće, dostaviti prema obrascu u Prilogu 2.

Dodatno, molimo da učesnici opišu:

- **Dimenzionisanje i licenciranje:** način dimenzioniranja i licenciranja, od kojeg momenta se počinju naplaćivati licence, te da li su licence trajne (perpetual) ili vremenski ograničene (term-based).
- **Obim podrške:** obim usluga podrške pri održavanju.

- **Detalji licenciranja:** jedinica licenciranja (fizička jezgra, vCPU, socket, čvor ili klaster) i način tretiranja hyper-threadinga; da li se licenciraju control plane i infrastrukturni čvorovi; uslovi za laboratorijska, test i DR okruženja (hladna ili topla rezerva); uslovi za edge lokacije i klastere sa jednim čvorom; koje su komponente uključene u osnovnu pretplatu, a koje se posebno naplaćuju (npr. registar slika, softverski definisana pohrana, service mesh, napredna sigurnost, upravljanje više klastera).
- **Prenosivost licenci:** da li je licenca vezana za hardver određenog proizvođača; mogućnost prenosa licenci pri zamjeni ili proširenju servera, te između klastera i lokacija; mogućnost odvojene nabavke hardvera i softvera.
- **Uslovi obnove i model plaćanja:** maksimalni rast cijene pri obnovi pretplate, popusti za višegodišnje ugovore te dostupni modeli plaćanja (pretplata, trajna licenca uz održavanje, plaćanje prema rastu kapaciteta).

Indikativne cijene traže se isključivo u informativne svrhe i ne predstavljaju obavezujuću ponudu.

PRILOG 1 – DETALJNA IZJAVA O USKLAĐENOSTI (SoC): ZAHTJEVI ZA TELCO-GRADE KUBERNETES PLATFORMU

Za svaki zahtjev u koloni „Usklađenost“ navesti: FC – potpuno usklađeno standardnom funkcionalnošću platforme; PC – djelimično usklađeno ili usklađeno uz dodatnu komponentu; NC – nije usklađeno; RM – planirano (navesti verziju i rok); N/A – nije primjenjivo na domenu učesnika (uz kratko obrazloženje). Tamo gdje zahtjev navodi konkretan alat ili parametar, prihvatljivo je i funkcionalno ekvivalentno rješenje, uz obrazloženje u koloni komentara. Zahtjevi koji se odnose na fizičku mrežnu topologiju i lokacije (3.9, 3.10, 3.11, 3.12, 6.15 i 6.16) tumače se u skladu s poglavljem 2.1: prihvatljive su i topologije sa najmanje dvije redundantne putanje te logičko (VLAN) razdvajanje mreža, a učesnici u komentaru navode svoju preporuku.

Ref.	Zahtjev	Usklađenost	Komentar dobavljača
1. Usklađenost i standardi			
1.1	Usklađenost sa ETSI GS NFV-IFA 011 (specifikacije VNF/CNF deskriptora), gdje je primjenjivo.		
1.2	Podrška za 3GPP-usklađenu izolaciju mrežnih slice-ova na nivou platforme (TS 28.530 / TS 28.531).		
1.3	Usklađenost sa najboljim praksama i referentnim arhitekturama CNCF telekom zajednice (Telecom User Group).		
1.4	Podrška za ETSI GS NFV-SOL 001/002 formate deskriptora radi interoperabilnosti.		

Ref.	Zahtjev	Usklađenost	Komentar dobavljača
1.5	Usklađenost sa NIST SP 800-190 (Application Container Security Guide) i NIST SP 800-204 (Security Strategies for Microservices).		
2. Osnovne funkcionalnosti			
2.1	Obaveza podrške Kubernetes verzija prema politici N-2.		
2.2	Podrška za opterećenja koja zahtijevaju povišene Linux capabilities, uključujući NET_RAW, NET_ADMIN, SYS_ADMIN (gdje je izričito dozvoljeno politikom).		
2.3	Podrška za Horizontal Pod Autoscaler (HPA) v2 sa custom i eksternim izvorima metrika.		
2.4	Podrška za Vertical Pod Autoscaler (VPA) za dimenzionisanje stateful CNF komponenti.		
2.5	Podrška za PriorityClasses i Preemption radi zagarantovanog raspoređivanja kritičnih CNF opterećenja.		
2.6	Podrška za Pod Topology Spread Constraints za raspoređivanje svjesno zona i rack-ova.		
2.7	Podrška za rolling nadogradnje bez prekida rada za stateless opterećenja.		
2.8	Podrška za node affinity, pod affinity i anti-affinity pravila.		
2.9	Podrška za CRD-ove i Operator obrazac za upravljanje životnim ciklusom CNF-ova.		
2.10	Instalacija Helm paketa bez cluster-admin privilegija – ograničeni RBAC mora biti dovoljan.		
2.11	Podrška za čuvanje Helm paketa u privatnom OCI registru.		
2.12	Podrška za Helm Secrets ili ekvivalent za upravljanje enkriptovanim vrijednostima, integrisano sa eksternim sistemom za tajne.		
2.13	Visoko dostupan control plane sa najmanje tri etcd člana i tri API server replike.		
2.14	Smještaj control plane-a na namjenske čvorove (odvojeno od CNF opterećenja).		

Ref.	Zahtjev	Usklađenost	Komentar dobavljača
2.15	Nadzor zdravlja etcd klastera sa automatskom defragmentacijom i kompakcijom.		
2.16	Enkripcija etcd-a u mirovanju ključevima AES-GCM ili AES-CBC 256-bit.		
2.17	API server audit logovanje sa podesivom audit politikom i rotacijom logova.		
2.18	Podrška za admission kontrolere za provođenje politika (OPA Gatekeeper, Kyverno ili ekvivalent).		
2.19	Podrška za ValidatingAdmissionWebhook i MutatingAdmissionWebhook za CNF-specifičnu validaciju.		
2.20	Izlaganje metrika control plane-a eksternim sistemima nadzora (Prometheus-kompatibilno).		
3. Hardver, mreža i pohrana			
3.1	Podrška za Kubernetes CPU Manager sa „static“ politikom za Guaranteed QoS podove.		
3.2	Ekskluzivni CPU pinning za CNF opterećenja osjetljiva na latenciju (npr. 5G DU, obrada RTP medija).		
3.3	NUMA-aware raspoređivanje putem Topology Manager-a („single-numa-node“ i „best-effort“ politike).		
3.4	Izolacija CPU jezgri putem kernel parametara (isolcpus, nohz_full, rcu_nocbs) za real-time CNF jezgre.		
3.5	Više grupa čvorova (node pools) sa različitim hardverskim profilima (opšti, high-performance, storage-optimizovani).		
3.6	Kubernetes Taints i Tolerations za strogu izolaciju opterećenja između grupa čvorova.		
3.7	Labele i selektori čvorova za raspoređivanje CNF-ova na odgovarajuće hardverske profile.		
3.8	Politike automatskog skaliranja grupa čvorova sa definisanim minimalnim i maksimalnim brojem čvorova.		

Ref.	Zahtjev	Usklađenost	Komentar dobavljača
3.9	Najmanje dvije redundantne mrežne putanje (poželjno tri) između računarskih čvorova i ToR switcheva (LACP bonding ili ekvivalent).		
3.10	Fizičko razdvajanje management, underlay, storage i CNF data-plane mreža. Prihvatljivo je i logičko (VLAN) razdvajanje.		
3.11	VLAN segmentacija kroz sve fizičke mrežne domene.		
3.12	ToR switchevi sa ECMP podrškom za raspodjelu opterećenja na uplink vezama.		
3.13	Produkcijski, CNCF-conformant CNI plugin. Npr. OVN-Kubernetes, Calico ili Cilium ili funkcionalno ekvivalentno rješenje.		
3.14	Provođenje NetworkPolicy (ingress i egress) na nivou poda i namespace-a.		
3.15	Kubernetes DNS (CoreDNS) sa prosljeđivanjem prilagođenih zona za interne telco domene.		
3.16	IPv4/IPv6 dual-stack mreža klastera.		
3.17	DSCP označavanje izlaznog saobraćaja podova radi integracije sa QoS politikama MPLS/IP transporta.		
3.18	Proširenje volumena (poželjno online, prihvatljivo offline) za rast stateful CNF-ova.		
3.19	Snapshot volumena (CSI VolumeSnapshot) za backup i restore.		
3.20	Garancija da SLA performansi pohrane nije ugrožen opterećenjima koja dijele infrastrukturu (QoS izolacija).		
4. Sigurnost			
4.1	Platforma se MORA isporučiti u ojačanom (hardened) stanju. Zadane permisivne konfiguracije nisu prihvatljive. Hardening se odnosi na OS, Kubernetes komponente i sve platformske usluge.		

Ref.	Zahtjev	Usklađenost	Komentar dobavljača
4.2	Platforma unaprijed ojačana i usklađena sa CIS Kubernetes Benchmarkom, odnosno CIS benchmarkom za konkretnu distribuciju (Level 1 minimum; Level 2 gdje je operativno izvodivo). Uz isporuku dostaviti izvještaj automatizovanog alata (kube-bench, compliance operator ili ekvivalent) za isporučenu verziju.		
4.3	Operativni sistem čvorova ojačan prema odgovarajućem CIS Benchmarku za odabrani OS (uključujući nepromjenjive, za kontejnere optimizovane OS). Uz isporuku dostaviti izvještaj skeniranja.		
4.4	Usklađenost sa NIST SP 800-190 i NIST SP 800-204 za sve dizajnerske odluke na nivou platforme.		
4.5	RBAC sa definicijama uloga na nivou namespace-a i klastera.		
4.6	Integracija sa eksternim Identity Provider-ima (IdP) putem OIDC-a za autentikaciju operatera (npr. Keycloak, LDAP bridge).		
4.7	Princip najmanjih privilegija – bez zadanih cluster-admin veza za CNF servisne naloge.		
4.8	Integracija sa HashiCorp Vault ili ekvivalentom za dinamičko ubacivanje tajni (External Secrets Operator, Vault Agent).		
4.9	Provođenje Pod Security Standards (PSS) ili strožijeg ekvivalentnog mehanizma platforme – Baseline ili Restricted profil kao zadani; Privileged samo gdje je izričito potrebno.		
4.10	Odbacivanje Linux capabilities (drop: ALL) uz izričito dodavanje samo potrebnih.		
4.11	Seccomp profili (RuntimeDefault ili prilagođeni) po podu/kontejneru.		
4.12	SELinux ili AppArmor profili za mandatory access control na osjetljivim CNF podovima.		
4.13	Admission kontroleri (OPA Gatekeeper, Kyverno ili ekvivalent) za provođenje sigurnosnih politika organizacije kao koda.		

Ref.	Zahtjev	Usklađenost	Komentar dobavljača
4.14	NetworkPolicies po zadanim postavkama – deny-all ingress/egress osnova sa izričitim allow pravilima po CNF-u.		
4.15	mTLS za komunikaciju CNF–CNF unutar klastera.		
4.16	Provjera potpisa kontejnerskih slika (Cosign / Notary v2) pri prijemu (admission).		
4.17	Integracija sa privatnim registrom kontejnerskih slika i upravljanje pull-secret-ima.		
4.18	Integrisano skeniranje ranjivosti kontejnerskih slika u registru.		
4.19	Kubernetes API audit logovanje sa podesivom politikom (nivoi Metadata / Request / RequestResponse).		
4.20	Prosljeđivanje audit logova u nepromjenjiv, na izmjene otporan eksterni SIEM ili sistem za upravljanje logovima.		
4.21	Audit trag pristupa operatera koji pokriva sve povlaštene operacije (exec, port-forward i sl.).		
4.22	Automatizovano ocjenjivanje usklađenosti sa CIS Benchmarkom (kube-bench, compliance operator ili ekvivalent).		
4.23	Onemogućen anonimni pristup resursima API servera; eventualni izuzeci ograničeni isključivo na health/discovery endpoint-e i dokumentovani.		
4.24	Uključen NodeRestriction admission plugin radi ograničenja kubelet dozvola.		
4.25	Autorizacija uključuje Node i RBAC; AlwaysAllow se NE SMIJE koristiti ni u jednom okruženju.		
4.26	Spriječena upotreba keširanih slika iz drugih namespace-ova (AlwaysPullImages admission kontroler ili ekvivalentna kontrola putem politike).		
4.27	Parametri čuvanja audit logova (starost, broj i veličina datoteka) podešeni za čuvanje od 90 dana.		

Ref.	Zahtjev	Usklađenost	Komentar dobavljača
4.28	Pristup API serveru ograničen na management mreže – Kubernetes API ne smije biti dostupan sa CNF data-plane mreža.		
4.29	etcd peer i client TLS sa obostranom autentikacijom.		
4.30	Pristup etcd-u ograničen isključivo na Kubernetes API server – bez direktnog pristupa sa radnih čvorova ili iz CNF podova.		
4.31	Enkripcija Secrets resursa u etcd-u (AES-GCM ili AES-CBC, 256-bit ključ) uz mogućnost upravljanja ključem putem eksternog KMS-a.		
4.32	etcd se izvršava izolovano, sa minimalnim privilegijama i minimalnim dozvolama nad direktorijem podataka (mode 700).		
4.33	Enkripcija ConfigMaps podataka u etcd-u, pored Secrets, gdje platforma to podržava.		
4.34	Onemogućene i uklonjene sve nepotrebne OS usluge i daemoni na čvorovima (npr. avahi, cups, rpcbind, bluetooth).		
4.35	SSH hardening na svim čvorovima: onemogućen root login i autentikacija lozinkom, SSH ograničen na management interfejse, obavezna autentikacija ključem.		
4.36	Filtriranje saobraćaja na nivou hosta (firewalld, nftables ili ekvivalentna kontrola platforme) na svim čvorovima – dozvoljen samo potreban Kubernetes i management saobraćaj.		
4.37	Spriječeno curenje informacija o procesima između CNF opterećenja (hidepid opcija za /proc ili ekvivalentna izolacija putem kontejnerskog runtime-a i SELinux-a ili ekvivalenta).		
4.38	Onemogućeno automatsko učitavanje nekorištenih i potencijalno opasnih kernel modula (npr. dccp, rds, tipc); SCTP mora ostati dostupan tamo gdje ga CNF-ovi zahtijevaju.		

Ref.	Zahtjev	Usklađenost	Komentar dobavljača
4.39	auditd na svim čvorovima sa pravilima za: izvršavanje povlaštenih komandi, izmjene dozvola datoteka, izmjene korisnika/grupa, izmjene mrežne konfiguracije i učitavanje kernel modula.		
4.40	ResourceQuota i LimitRange na svim nesistemskim namespace-ovima radi sprječavanja iscrpljivanja resursa od strane jednog CNF-a.		
4.41	kube-system i ostali platformski namespace-ovi nedostupni CNF servisnim nalozima putem RBAC-a.		
4.42	Zadana deny-all NetworkPolicy automatski primijenjena na sve novokreirane namespace-ove (admission webhook, šablon projekta ili GitOps politika).		
4.43	Zasebni namespace-ovi po proizvođaču CNF-a i po CNF funkciji kao minimalna granica izolacije.		
4.44	LimitRange zadane vrijednosti na nivou namespace-a, tako da i kontejneri bez izričitih requests/limits dobiju ograničene resurse.		
4.45	Bez čuvanja kredencijala, tokena ili certifikata u čistom tekstu u ConfigMaps – svi osjetljivi podaci koriste Kubernetes Secrets ili eksterni sistem za tajne.		
4.46	Pristup Secrets ograničen putem RBAC-a – CNF servisni nalozi imaju pristup samo izričito potrebnim Secret objektima u vlastitom namespace-u (bez wildcard naziva resursa).		
4.47	Integracija sa eksternim sistemom za upravljanje tajnama (HashiCorp Vault, CyberArk) tako da se tajne nikada ne čuvaju u Git repozitorijima u čistom tekstu.		
5. Metrike, logovanje i alarmiranje			
5.1	Prometheus-kompatibilne metrike za sve komponente platforme (API server, etcd, kubelet, CNI, CSI).		

Ref.	Zahtjev	Usklađenost	Komentar dobavljača
5.2	Isporučen ili integrisan Prometheus stack (Prometheus Operator ili Thanos za dugoročno čuvanje).		
5.3	Unaprijed pripremljena pravila alarmiranja za narušavanje SLO-a platforme (nedostupnost čvora, OOMKill poda, etcd latencija, pun PVC).		
5.4	Custom metrics adapteri (Prometheus Adapter ili ekvivalent) za HPA v2 skaliranje prema poslovnim metrikama CNF-a.		
5.5	Grafana ili ekvivalentni dashboard-i, sa unaprijed pripremljenim prikazima stanja klastera, čvorova i opterećenja.		
5.6	Kontrole kardinalnosti metrika radi sprječavanja preopterećenja Prometheusa.		
5.7	Platformski upravljano rješenje za agregaciju logova (npr. Loki, OpenSearch, Vector, Fluentd/Fluent Bit).		
5.8	Strukturirano logovanje (JSON) svih komponenti platforme.		
5.9	Prosljeđivanje logova u eksterni SIEM (syslog, Kafka ili Elasticsearch-kompatibilan endpoint).		
5.10	Čuvanje logova najmanje 90 dana, na klasteru ili van njega, uz mogućnost pretrage.		
5.11	Alertmanager (ili ekvivalent) sa podesivim pravilima rutiranja, grupisanja i potiskivanja.		
5.12	Prosljeđivanje alarma u NOC alate operatera putem webhook-a.		
5.13	Alarmiranje zasnovano na otkrivanju anomalija radi proaktivnog sprječavanja incidenata.		
5.14	Podrška za cert-manager za automatizovano upravljanje životnim ciklusom X.509 certifikata.		
5.15	Integracija cert-manager-a sa ACME i Vault PKI Secrets Engine.		
6. Životni ciklus i operacije			
6.1	Potpuno automatizovana, ponovljiva instalacija klastera iz Infrastructure-as-Code (Terraform, Ansible ili ekvivalent proizvođača).		

Ref.	Zahtjev	Usklađenost	Komentar dobavljača
6.2	Instalacija u air-gapped / mrežno ograničenom okruženju, sa svim artefaktima dostupnim kao offline paket (slike, Helm paketi, OS paketi).		
6.3	Multi-tenancy zasnovan na namespace-ovima sa kvotama resursa i LimitRange po CNF-u.		
6.4	Samouslužno kreiranje namespace-ova za CNF timove putem GitOps tokova.		
6.5	Validiran vodič za uvođenje CNF-ova koji pokriva RBAC, NetworkPolicy, StorageClass i admission politike.		
6.6	Rolling nadogradnja Kubernetes control plane-a bez prekida rada klastera.		
6.7	Rolling nadogradnja radnih čvorova uz poštivanje PodDisruptionBudget-a (drain → upgrade → rejoin).		
6.8	Drain i cordon čvora bez uticaja na aktivna CNF opterećenja.		
6.9	Sigurnosno ažuriranje OS-a sa automatizovanim uvođenjem i mogućnošću povrata (rollback).		
6.10	Blue/green nadogradnje klastera – paralelno podizanje klastera sa prebacivanjem saobraćaja.		
6.11	Kanarinske nadogradnje čvorova – nadogradnja podskupa čvorova prije uvođenja na cijelu flotu.		
6.12	Automatizovano otkrivanje odstupanja CRD-ova i Helm release-a uz usklađivanje putem GitOps-a.		
6.13	Self-healing platforme: automatsko otkrivanje i oporavak/zamjena čvora pri hardverskom kvaru.		
6.14	Prediktivna upozorenja za održavanje zasnovana na trendovima hardverske telemetrije (poželjno).		
6.15	Podrška za najmanje tri fizičke zone dostupnosti, svaka sa nezavisnim napajanjem, hlađenjem i mrežnim putanjama. Prihvatljiv je i dizajn sa manjim brojem zona dostupnosti, uz opis načina postizanja otpornosti		

Ref.	Zahtjev	Usklađenost	Komentar dobavljača
6.16	Raspored control plane čvorova po zonama dostupnosti – najviše jedan control plane čvor po zoni. Prihvatljiv je i dizajn sa manjim brojem zona dostupnosti, uz opis načina postizanja otpornosti		
6.17	Anti-affinity na nivou rack-a za raspoređivanje kritičnih CNF podova.		
6.18	Redundansa mrežnih putanja – gubitak jedne fizičke veze ne smije uzrokovati prekid servisa.		

Odgovore je potrebno dostaviti u pisanoj formi, strukturirane prema numeraciji poglavlja ovog dokumenta (poglavlja 2 i 4), uz popunjenu matricu iz poglavlja 3.1 i izjavu o usklađenosti iz Priloga 1. Rok, način i adresa za dostavu odgovora navedeni su u službenoj objavi ovog zahtjeva. Sva pitanja i zahtjeve za pojašnjenje potrebno je uputiti putem standardnih kanala komunikacije BH Telecoma. Ovaj RFI ima isključivo informativni karakter i ne predstavlja poziv za dostavu ponuda niti obavezu BH Telecoma da pokrene postupak nabavke. Troškove pripreme odgovora snose učesnici. Informacije koje smatraju povjerljivim učesnici trebaju jasno označiti u svojim odgovorima.

PRILOG 2 – OBRAZAC ZA INDIKATIVNE CIJENE

Molimo učesnike da indikativne cijene iz poglavlja 4.8, gdje je moguće, iskažu u sljedećem obrascu. Moguće je i cijenovni obrazac prilagoditi, prema ponuđenom tehničkom rješenju. Cijene iskazati bez PDV-a, u EUR i BAM. Stavke koje se ne odnose na domenu učesnika označiti kao „N/A“, a dodatne stavke navesti na kraju tabele.

Naziv učesnika: _____ Datum cijena: _____ Važnost do: _____

Rb.	Stavka	Jedinica mjere	Jednokratno (CAPEX) EUR	Jednokratno (CAPEX) BAM	Godišnje (OPEX) EUR	Godišnje (OPEX) BAM	Napomena
1	Serverski profil – control plane čvor	po serveru					specifikacija, garancija
2	Serverski profil – opšti radni čvor	po serveru					specifikacija, garancija
3	Serverski profil – high-performance	po serveru					specifikacija, garancija

	radni čvor (SR-IOV/DPDK)						
4	Mrežna oprema (ToR switchevi i sl.)	po komadu					
5	Kubernetes/CaaS platforma	po jedinici licenciranja					navesti jedinicu licenciranja
6	Dodatne licence i pretplate	po komponenti					registar, SDS, service mesh, sigurnost i dr.
7	Instalacija i integracija	paušal / čovjek-dan					
8	Podrška i održavanje – standardni nivo	godišnje					vremena odziva
9	Podrška i održavanje – 24x7 / premium	godišnje					vremena odziva
10	Nadogradnje i migracije	paušal / čovjek-dan					
11	Rezervni kapacitet i disaster recovery	po čvoru / klasteru					hladna / topla rezerva
12	Obuka i prenos znanja	po učesniku / grupi					
13	Stručne usluge (dnevnica po profilu inženjera)	čovjek-dan					navesti profile
	Ukupno – godina 1						
	TCO – 3 godine						navesti pretpostavke

	TCO – 5 godina						navesti pretpostavke

Indikativne cijene traže se isključivo u informativne svrhe i ne predstavljaju obavezujuću ponudu.