

Príloha č. 1 Výzvy: Opis predmetu zákazky

Predmetom zákazky je dodanie softvérových komponentov v špecifikácii, počte a rozsahu uvedenom v tabuľkách nižšie vrátane poskytnutia súvisiacich služieb dodania tovaru do miesta dodania, vyloženia tovaru v mieste dodania, odberu a ekologickej likvidácia spotrebného materiálu/obalov, ako aj poskytnutie súčinnosti pri inštalácii a konfigurácii, inštalácii ovládačov, poskytnutia telefonической podpory a záruky na mieste v trvaní uvedenom pri jednotlivých položkách predmetu zákazky.

Predmetom ponuky musia byť nové, doposiaľ nepoužívané softvérové komponenty a ich podpora musí byť poskytovaná priamo výrobcom softvérových komponentov.

Softvérové komponenty

Softvér pre prevádzku, hromadnú správu a zabezpečenie distribuovaných prostredí pre poskytovanie PaaS funkcionalít a prevádzkovanie kontajnerovaných aplikácií (Kubernetes Platforma)

Verejný obstarávateľ požaduje dodanie softvérového balíka pre prevádzku, hromadnú správu a zabezpečenie distribuovaných prostredí pre poskytovanie PaaS funkcionalít a prevádzkovanie kontajnerovaných (Linux i Windows kontajnerov) aplikácií, vrátane dodania služieb podpory od výrobcu pre softvérový produkt.

Verejný obstarávateľ požaduje uviesť cenu za minimálny pack a cenu pre **192 vCPU kontajnerovej platformy a 16 vCPU pre integračnú a streamovaciu platformu.**

Technické vlastnosti	Minimálne požadované parametre
Požiadavky na dodanie softvérového produktu	Samoobslužná platforma pre vývojárov aplikácií, ktorá umožňuje vytvárať a prevádzkovať aplikácie v Linux a Windows kontajneroch,
	Platforma musí umožňovať automatické škálovanie prevádzkovaných aplikácií,
	platforma musí mať klastrovú vrstvu služieb pre Linuxové a Windows kontajnery, ktorá zabezpečí ich vysokú dostupnosť a rozloženie záťaže,
	musí umožňovať automatizáciu činností ako je prideľovanie zdrojov, či systémová správa platformy,
	musí umožňovať správu platformy pomocou príkazového riadku, web konzoly a integrovaných vývojárskych prostredí,
	musí mať integrovaný register kontajnerov so samostatnými repozitármi pre rôzne aplikácie (separácia images per app), musí umožňovať nastavovanie vlastných pravidiel (napr. mazanie starších image podľa definovaných pravidiel či "garbage collection"),
	musí mať integrovaný katalóg služieb

	Integrovaný marketplace pre rozšírenie platformy o ďalšie funkcionality
	musí umožňovať jednoduchý “debugging” kontajnerových aplikácií bežiacich v klastri.
	musí umožňovať updatovanie softvérového produktu bez výpadku služieb prevádzkovaných v spustených kontajneroch,
	musí umožňovať updatovanie aplikácií prevádzkovaných v spustených kontajneroch bez výpadku služieb nimi poskytovaných,
	musí poskytovať webové služby (API) pre integráciu s CI/CD nástrojmi ako GitLab,
	musí poskytovať nástroje pre vytváranie a testovanie kontajnerov,
	musí poskytovať nástroje pre centralizované nasadzovanie aplikácií,
	autentifikácia používateľov softvérového produktu musí umožňovať integráciu s Active Directory,
	autentifikácia používateľov softvérového produktu musí podporovať SSO pre integráciu s viacerými identifikačnými autoritami,
	musí poskytovať API pre zálohovanie a obnovu aplikácií (vrátane ich nastavenia) v klastri vrátane ich perzistentných dát,
	musí umožňovať zálohovanie konfigurácie a obnovu do pôvodného stavu v prípade poruchy,
	musí mať integrované role a umožňovať pridelovanie rôznych úrovní práv na rôzne časti platformy týmto roliam, musí mať samostatnú rolu umožňujúcu monitorovanie kontajnerov a tiež samostatné role pre nasadzovanie kontajnerov, musí umožňovať prístup len k niektorým repozitárom v registry, s rôznymi právami (čítanie images, zápis images),
	musí umožňovať audit a logovanie zmien (najmä zmien v registri images a tiež deploymentov a rollbackov), musí umožňovať vytváranie a prezentáciu reportov v UI,
	musí mať integrovaný natívny kontajner storage s nasledovnými vlastnosťami: · dopĺňa celkové riešenie o vrstvu softvérovo definovaného úložiska dát (storage), · poskytuje perzistentné úložisko dát pre kontajnery, · poskytuje automatickú dynamickú škálovateľnosť perzistentného storage pre kontajnery, · umožňuje vývojárom aplikácií pridávať, či meniť veľkosť perzistentného storage bez nutnosti zásahu zo strany správcu platformy, · poskytuje vysokú dostupnosť storage rovnako ako ostatné súčasti platformy,

	musí mať integrovaný systém pre zber a zobrazovanie systémových a aplikačných logov,
	musí mať integrovaný systém pre zber a zobrazovanie systémových a aplikačných metrik,
	musí umožňovať spúšťanie alertov na základe administrátorom špecifikovaných pravidiel,
	musí podporovať CPU architektúry x86 a ARM,
	musí byť on-premise riešenie, ktoré bude celé realizované v dátových centrách obstarávateľa.
	Musí podporovať automatizovanú inštaláciu do public cloudov ako AWS, Microsoft Azure, Google Cloud Platform, Microsoft Azure Government, bare metal, Red Hat OpenStack Platform, VMware vSphere.
Požiadavky na vytváranie, nasadzovanie a beh aplikácií	Softvérový produkt poskytuje užívateľské prostredie určené pre vývojárov, umožňujúce jednoduchým spôsobom sledovať topológiu aplikácie, stav vytvárania a nasadenia aplikácie.
	Softvérový produkt poskytuje užívateľské prostredie zamerané na správu produktu.
	Softvérový produkt poskytuje vývojové prostredie (IDE) v prehliadači.
	Softvérový produkt umožňuje jednoduchý prevádzku prostredia pre chod serverless (FaaS).
	Softvérový produkt umožňuje vytvárať a nasadzovať kontajnery na základe zdrojového kódu aplikácie dostupného zo systému s verziovaním, napríklad git.
	Poskytuje nástroje pre Monitoring aplikácií a ich custom metriky.
	Poskytuje nástroje pre zber a zobrazovanie systémových a aplikačných logov.
Požiadavky na správu platformy (Day 2 operations)	Softvérový produkt umožňuje automatické škálovanie aplikácií.
	Možnosť Inštalácie na Bare Metal servery, Virtuálne servery a do public cloud prostredí.
	Softvérový produkt umožňuje automatické škálovanie prevádzkovaných klastrov.
	Upgrade Softvérového produktu je plne automatizovaný.
Požiadavky na Multiklaster	Softvérový produkt je nezávislý na jedinom dodávateľovi HW/SW pre úložisko a sieťové prvky.
	Centralizovaná správa plne automatizovaného vytvárania nových klastrov.

	Centralizovaná správa upgrade spravovaných klastrov.
	Centralizované kontinuálne nasadzovanie do skupiny klastrov pre dané prostredie (napr. test, preprod, či prod), ktoré je vizualizované v UI.
	Centralizovaná správa nastavenie bezpečnostných politik.
	Centralizovaný monitoring spravovaných klastrov.
	Centralizovaný monitoring dashboard .
	Centralizovaná správa nastavenie bezpečnostných politik.
	Centralizovaný monitoring spravovaných klastrov.
	Dynamické vyhľadávanie pre zobrazovanie a investigáciu aplikácií naprieč spravovanými klastrami.
	Automatizovaná analytika softvérového produktu, ktorá proaktívne kontroluje stav klastrov a navrhuje opravné kroky.
	Centralizované nastavenie internej sieťovej komunikácie medzi klastrami na rôznych platformách.
	Centralizovaná správa obsahuje politiky pre nastavenie bezpečnosti, odolnosti, a konfiguračnej správy.
Požiadavky na bezpečnosť	Platforma zobrazuje zraniteľnosti v aktuálne bežiacich kontajneroch.
	Governance a risk dashboard, ktorá zobrazuje bezpečnostné riziká a porušenia predpísaných bezpečnostných politik.
	Hromadná správa bezpečnostných politik skupiny klastrov.
	Integrácia s Open Policy Agent (OPA) pre rozšírenie bezpečnostných a iných politik.
	Poskytuje pohľad na aplikácie, ich kontajnerové image a nastavenia z hľadiska bezpečnosti.
	Zobrazuje sieťovú komunikáciu medzi viacerými prostrediami v klastrí.
	Navrhuje pravidlá pre zabezpečenie sieťovej komunikácie v klastrí.
	Bezpečnostný systém je schopný detekovať anomálne chovanie aplikácií ako napríklad malware, ťažba kryptomien, alebo pokus o neautorizovaný prístup k citlivým údajom.
	Systém, ktorý monitoruje kontajnerovú platformu z hľadiska bezpečnosti, je integrovateľný so SIEM systémami.
	Obsahuje politiky pre kontrolu pri vytváraní a nasadzovaní kontajnerových image z hľadiska známych zraniteľností.

	Obsahuje prehľadný dashboard stavu compliance klastrov pre potreby auditu.
	Vizualizuje povolenú a zakázanú sieťovú komunikáciu a doporučuje úpravu sieťovej komunikácie pre odobratie nadbytočných sieťových oprávnení.
	Analýza oprávnení prístupu k citlivým informáciám.
	Bezpečnostný softvér poskytuje API pre integráciu s externými DevOps systémami, zahrňujúcimi CI/CD nástroje, skenovanie image a SIEM (security integration event management) riešeniami.
	Ponúka kontajnerovú base image, čím zaručuje podporu a updaty.
Požiadavky na Integráciu	Musí podporovať tvorbu a správu klastrov pre Stream Messaging, ako napr. Apache Kafka.
	Musí podporovať governance APIs, ako je API dokumentácia, API schéma, API poskytovateľa, API konzumenti. Taktiež musí podporovať správu API, ako sú prevádzkové parametre, verzovanie, logy, metriky, alerty U API musí podporovať implementáciu, teda Developer portál, API katalog, sdk, Mock APIs.
	Musí podporovať prevádzku aplikačných serverov i aplikačných frameworkov zameraných na mikroslužby, vrátane podpory reaktívneho vývoja pre vytváranie distribuovaných aplikácií.
Požiadavky na dodanie podpory výrobcu pre softvérový produkt	Podpora priamo od výrobcu dodávaného softvérového produktu,
	dĺžka podpory 3 roky od prevzatia.
	nárok na aktuálne verzie softvérového produktu, prístupné prostredníctvom portálu výrobcu,
	prístup k opravným balíkom,
	podpora poskytovaná v rozsahu 8 hodín denne v rozmedzí 9:00 – 17:00 SEČ, v pracovných dňoch,
	podpora poskytovaná telefonicky, formou emailu, alebo cez ticketovací portál výrobcu.
	prístup k dokumentácii prostredníctvom webového portálu výrobcu,
	prioritizácia riešenia nahlásených prípadov podpory podľa ich dopadu na celkovú funkčnosť softvérového produktu,

	doba odozvy pre príslušnú úroveň závažnosti musí byť garantovaná v nasledujúcom rozsahu: Závažnosť 1. úrovne – kritická Produkt nie je použiteľný, čo vedie k celkovému narušeniu práce, alebo k inému závažnému dopadu na prevádzku. Reakčná doba: 1 hodina, Závažnosť 2. úrovne – vysoká Zlyhanie veľmi dôležitej čiastkovej funkčnosti produktu. Prevádzka je vážne obmedzená. Reakčná doba: 4 hodiny, Závažnosť 3. úrovne – nízka Zlyhanie menej dôležitej čiastkovej funkčnosti produktu. Produkt nefunguje podľa špecifikácií stanovených výrobcom. Prevádzka je obmedzená len čiastočne. Reakčná doba: 1 pracovný deň, Závažnosť 4. úrovne – iná Nezávažný problém. Môže to byť napr. žiadosť o dokumentáciu, všeobecnú informáciu, žiadosť o vylepšenie a pod. Reakčná doba: 2 pracovné dni.
--	---

Softvér pre automatizáciu IaaS

Verejný obstarávateľ požaduje dodanie softvérového balíka pre prevádzku, správu a zabezpečenie nekontajnerovanej infraštruktúry pre poskytovanie IaaS funkcionalít, vrátane dodania služieb podpory od výrobcu pre softvérový produkt.

Verejný obstarávateľ požaduje uviesť cenu za minimálny pack a cenu pre **200 VM**

Požiadavky na dodanie softvérového produktu	Možnosť spúšťať automatizačné úkony a skripty, ktoré nastavujú nekontajnerizovanú infraštruktúru mimo softvérový produkt, ako sú napríklad sieťové prvky, úložisko, DNS, či Load Balancery.
	Možnosť použitia aj pri nasadzovaní a upgrade aplikácií alebo na nápravu klastrov ktoré niesú compliant.
	Možnosť nasadenia a spúšťania z kontajnerovej platformy
Požiadavky na dodanie podpory výrobcu pre softvérový produkt	Podpora priamo od výrobcu dodávaného softvérového produktu,
	dĺžka podpory 3 roky od prevzatia.
	nárok na aktuálne verzie softvérového produktu, prístupné prostredníctvom portálu výrobcu,
	prístup k opravným balíkom,
	podpora poskytovaná v rozsahu 8 hodín denne v rozmedzí 9:00 – 17:00 SEČ, v pracovných dňoch,
	podpora poskytovaná telefonicky, formou emailu, alebo cez ticketovací portál výrobcu.

	prístup k dokumentácii prostredníctvom webového portálu výrobcu,
	prioritizácia riešenia nahlásených prípadov podpory podľa ich dopadu na celkovú funkčnosť softvérového produktu,
	doba odozvy pre príslušnú úroveň závažnosti musí byť garantovaná v nasledujúcom rozsahu: Závažnosť 1. úrovne – kritická Produkt nie je použiteľný, čo vedie k celkovému narušeniu práce, alebo k inému závažnému dopadu na prevádzku. Reakčná doba: 1 hodina, Závažnosť 2. úrovne – vysoká Zlyhanie veľmi dôležitej čiastkovej funkčnosti produktu. Prevádzka je vážne obmedzená. Reakčná doba: 4 hodiny, Závažnosť 3. úrovne – nízka Zlyhanie menej dôležitej čiastkovej funkčnosti produktu. Produkt nefunguje podľa špecifikácií stanovených výrobcom. Prevádzka je obmedzená len čiastočne. Reakčná doba: 1 pracovný deň, Závažnosť 4. úrovne – iná Nezávažný problém. Môže to byť napr. žiadosť o dokumentáciu, všeobecnú informáciu, žiadosť o vylepšenie a pod. Reakčná doba: 2 pracovné dni.

Softvér pre zálohovanie 1

V tabuľke nižšie sú uvedené požiadavky na softvér pre zálohovanie - požiadavky pre Backup (VM); verejný obstarávateľ požaduje uviesť cenu za minimálny pack a cenu **pre 200 VM**

Technické vlastnosti	Minimálne požadované parametre
Architektúra	Zálohovací SW musí pracovať s infraštruktúrou VMware založenou na verziách vSphere od 6.7, až po 7.0U3, vrátane VMware Cloud on AWS, VMware cloud on Dell EMC a Azure VMware Zálohovací software musí pracovať s infraštruktúrou MS Hyper-V 2012 R2, Hyper-V 2016 a Hyper-V 2019, až po Microsoft Windows Server Semi-Annual Channel (verzie 1803 až 20H2), ako aj Azure Stack HCI OS Riešenie musí byť HW nezávislé a musí byť možné ho prevádzkovať na fyzickej, virtuálnej i cloudovej infraštruktúre. Pre splnenie funkčných požiadaviek nesmie vyžadovať žiaden proprietárny HW, alebo proprietárny súborový systém. Riešenie nesmie byť licenčne obmedzené z pohľadu objemu zálohovaných dát na zdroji ani na cieľi. Design riešenie musí umožňovať automatizované zálohovanie v súlade s pravidlom pre ochranu dát 3-2-1 Riešenie musí umožňovať uchovávanie nezmeniteľnej (immutable) kópie dát na lokálnych diskových aj páskových (WORM) zariadeniach, aj v S3 objektových lokálnych i cloudových úložiskách

	Riešenie musí podporovať zálohovanie pre VMware vsphere aj MS Hyper-V prostredia s využitím LAN i SAN sietí Riešenie umožňuje využitie LTO páskovej knižnice pripojenej do FC SAN siete. Riešenie nesmie byť funkčne obmedzené len na zálohovanie virtualizovaných prostredí VMware vSphere a MS Hyper-V, ale musí umožňovať zálohovanie minimálne 2 ďalších hypervizorových platforiem, public cloud platforiem ako aj fyzických serverov a pracovných staníc a to minimálne s podporou OS Windows, Linux, AIX, Solaris a MacOS. Software musí umožňovať vytváranie záloh pomocou integrácie so snímkami diskového úložiska. Ďalej musí umožniť obnovu jednotlivých VM, súborov a položiek aplikácie z týchto snímok. Proces zálohy nesmie vyžadovať k pripojeniu snímky použité dočasného hostiteľa. Popísaná funkcia musí fungovať pre prostredia VMware vSphere a musí podporovať minimálne nasledujúcich výrobcov: HPE, Dell EMC, NetApp, Cisco, IBM, Lenovo, Fujitsu, Huawei, INFINIDAT, Pure Storage, DataCore Software musí byť schopný integrácie s inými systémami pomocou zabudovaného rozhrania REST API Software musí mať architektúru klient / server s možnosťou inštalácie viac inšancií administratívnej konzoly Riešenie nesmie byť licenčne obmedzené z pohľadu počtu a typu diskových, páskových, či cloudových úložísk záloh, či škálovateľnosti iných komponentov zálohovacej infraštruktúry pre dosiahnutie požadovaného výkonu, kapacity, alebo topológie zálohovacieho riešenia. Riešenie musí disponovať technológiu umožňujúcou rozširovanie kapacity úložiska záloh za plnej prevádzky Software musí podporovať hostiteľov spravovaných serverom VMware vCenter Server a samostatných hostiteľov. Software musí podporovať zálohovanie všetkých operačných systémov, ktoré sú podporované pre VMware alebo Hyper-V Jednotná správa riešenia nesmie byť závislá na žiadnom internetovom prehliadači.
Zálohovanie	Zálohy hypervizorových platforiem musia byť vytvárané na úrovni snímkov jednotlivých VM. Zálohovací mechanizmus musí disponovať nástrojmi na redukciu objemu dát ukladaných v súboroch záloh, typu kompresia a/alebo deduplikácia. Pokiaľ zálohovaný hypervizorová platforma podporuje mechanizmus pre sledovanie zmien dátových blokov, musí ju vedieť navrhované riešenie využívať. Zálohovacie úlohy musí byť možné definovať pre fixne definované objekty, fixnú, alebo dynamickú skupinu objektov na úrovni virtuálnych strojov, hostov, klastrov, diskových úložísk (Volumes, Datastores), alebo štítkov (vSphere Tags) Zálohovacie úlohy musí byť možné spúšťať automaticky v definovaných intervaloch, alebo ad-hoc ručne. Zálohovanie virtualizovaného prostredia nesmie vyžadovať inštaláciu a konfiguráciu zálohovacích agentov na úrovni GuestOS. Pripúšťa sa výnimka pri zálohovaní aplikačných klastrov rozprestretých cez viacero VM. Riešenie musí zaisťovať aplikačne konzistentné zálohy minimálne pre nasledovné aplikácie: MS Active Directory, MS Exchange, MS

	SharePoint, MS SQL, Oracle DB, PostgreSQL Pre MS SQL a OracleDB musí riešenie poskytovať i zálohovanie transakčných a archívnych logov. Riešenie musí disponovať mechanizmami na riadenie záťaže vytváranej zálohovacími úlohami na produkčnom prostredí a to minimálne na úrovni sietí a úložísk produkčných dát VMware a Hyper-V klastrov. Riešenie musí umožňovať vytváranie záloh s GFS retenčnou politikou na diskové, páskové médiá i cloudové úložiská Zálohovanie musí umožňovať vytváranie syntetických plných záloh s využitím BlockClone API v prípade ukladania súborov záloh na ReFS súborový systém. V prípade ukladania súborov záloh na súborový systém XFS sa predpokladá možnosť využitia ekvivalentnej funkcie Reflink V rámci zálohovacej úlohy musí byť možné definovať pre- a post-backup skripty, ako aj pre-freez a post-thaw skripty pre zaistenie aplikačnej konzistencie, alebo modifikáciu zálohovacieho prostredia. Riešenie musí disponovať mechanizmom na šifrovanie celej sieťovej prevádzky medzi všetkými komponentami a tiež šifrovaním "na cieľ" záložných súborov v úložisku súborov záloh minimálne na úrovni AES-256 Software musí podporovať granulárnu obnovu databáz Oracle s obnovou v čase (PIT) a podporu Oracle DataGuard pre databázy spustené v operačných systémoch Windows a Linux Software musí umožňovať publikovanie MS SQL a Oracle DB priamo zo záložného súboru na spustený databázový server Software musí umožňovať okamžitú obnovu databáz MS SQL a Oracle v režime Instant Recovery do ľubovoľného umiestnenia Software musí umožňovať integráciu natívneho pluginu pre zálohovanie Oracle RMAN Software musí umožňovať integráciu natívneho pluginu pre zálohovanie SAP HANA a SAP on Oracle (linux) Software musí umožňovať „reverzný CBT“ a obnovu pomocou Direct SAN Software musí umožňovať okamžitú obnovu záloh fyzických Windows a Linux OS na vSphere, alebo Hyper-V platformu s automatickou konverziou do zvoleného VM formátu. Riešenie musí disponovať mechanizmom na indexovanie súborových systémov GuestOS pre fulltextové vyhľadávanie. V rámci zálohovacej úlohy musí byť možné definovať poradie zálohovania jednotlivých VM. Riešenie musí umožňovať vytváranie súborov záloh pre každú VM samostatne Súbory záloh musia byť jednoducho migrovateľné na iný HW, napr. v prípade obmeny HW infraštruktúry. Nesmú byť závislé na žiadnej databáze, ktorej poškodenie by znemožnilo obnovu zálohovaných dát. Software musí mať replikáciu produkčných VM priamo z infraštruktúry VMware vSphere, medzi hosťiteľmi ESXi, vrátane asynchronej nepretržitej replikácie. Software musí umožniť ako zdroj replikačných úloh využiť súbory záloh
Obnoviteľnosť	Riešenie musí umožniť okamžitú obnovu VM jednotlivo, alebo v definovaných skupinách priamo zo súborov záloh. Riešenie musí umožniť okamžitú obnovu jednotlivých virtuálnych

	diskov priamo zo súborov záloh. Riešenie musí umožniť okamžitú obnovu MS SQL a Oracle DB databázy priamo zo súboru zálohy Obnova jednotlivých VM musí byť možná aj v prípade nefunkčnosti, alebo nedostupnosti zálohovacieho servera Zo zálohy VM musí byť možné obnoviť celú VM, jednotlivé virtuálne disky, súbory a adresáre súborového systému GuestOS, ako aj jednotlivé objekty aplikácií bez nutnosti inštalácie agentov do GuestOS pre obnovu. Pre všetky obnovy dát platí, že musí byť možnosť obnovy do pôvodnej, alebo inej lokality. Pre obnovy VM platí, že musí byť možné ich obnoviť aj na iných hypervizorových platformách, než na ktorých boli zálohované a/alebo priamo do prostredia verejného cloudu. Riešenie musí umožňovať pri obnove VM a jednotlivých virtuálnych diskov antimalware kontrolu obnovovaných dát Riešenie musí umožňovať obnovu dát v súlade s právom na výmaz osobných údajov v súlade s GDPR Riešenie musí umožňovať obnovu dát Active Directory na úrovni jednotlivých objektov, vrátane užívateľov, skupín, zariadení, Group Policy Objects, Integrated DNS a podobne. Riešenie musí umožňovať obnovu dát MS Exchange na úrovni objektov e-mail, kontakt, úloha, a podobne do lokálnej inštancie, alebo do prostredia Exchange online v rámci Office365 organizácie Obnova jednotlivých databáz MS SQL a Oracle DB musí byť možná k ľubovoľnému bodu v čase zo záloh transakčných a archívnych logov. Možnosť obnovy dát nesmie vyžadovať oprávnenia k prístupu na zálohovací server RBAC (Role-Based Access Control) musí umožňovať definovanie oprávnení pre užívateľov, alebo skupiny užívateľov pre obnovu dát minimálne na úrovni VM, GuestOS súbory a adresáre, MS SQL a Oracle DB databázy. Software musí mať samoobslužný portál, prostredníctvom ktorého si užívatelia môžu obnoviť súbory, virtuálne počítače, objekty MS Exchange a databázy MS SQL, databázy Oracle (vrátane obnovy v čase) Riešenie musí umožňovať automaticky priradovať politiky/pravidlá minimálne na základe TAGs, Labels, alebo názvov aplikácií Riešenie musí podporovať granularne RPO menej než 10 min Riešenie musí podporovať failover medzi regiónmi, zónami dostupnosti, naprieč cloudmi Podpora kompresie a deduplikácie S3/NFS cieľov Riešenie musí podporovať aplikačne konzistentné, databázovo konzistentné, a crash consistentné zálohy Požadujeme podporu polyglot persistencie
Bezpečnosť	Riešenie musí disponovať logikou na správu a riadenie životného cyklu šifrovacích kľúčov a hesiel. Riešenie musí disponovať automatickým mechanizmom overovania obnoviteľnosti záloh VM, vrátane testovania funkčnosti aplikačnej vrstvy s automatickým zasielaním výslednej detailnej správy z testu. Riešenie musí mať mechanizmus automatického overovania vadných dátových blokov a ich korekcie na úložisku záloh.

	Riešenie musí disponovať mechanizmom hlásenia chýb minimálne na úrovni notifikácií e-mailom a zasielania SNMP trapov do centrálneho dohľadového systému. Riešenie musí poskytovať možnosť zasielania hlásení do centrálnych dohľadových systémov minimálne cez SNMP protokol Riešenie musí poskytovať kontrolu zaplnenia úložísk pre ukladanie záloh s varovným hlásením pri dosiahnutí nastaviteľnej hodnoty. Riešenie musí mať vlastný mechanizmus zálohovania svojej konfigurácie s možnosťou šifrovania tejto zálohy
Požiadavky na dodanie podpory výrobcu pre softvérový produkt	Podpora priamo od výrobcu dodávaného softvérového produktu,
	dĺžka podpory 3 roky od prevzatia.
	nárok na aktuálne verzie softvérového produktu, prístupné prostredníctvom portálu výrobcu,
	prístup k opravným balíkom,
	podpora poskytovaná v rozsahu 8 hodín denne v rozmedzí 9:00 – 17:00 SEČ, v pracovných dňoch,
	podpora poskytovaná telefonicky, formou emailu, alebo cez ticketovací portál výrobcu.
	prístup k dokumentácii prostredníctvom webového portálu výrobcu,
	prioritizácia riešenia nahlásených prípadov podpory podľa ich dopadu na celkovú funkčnosť softvérového produktu,
	doba odozvy pre príslušnú úroveň závažnosti musí byť garantovaná v nasledujúcom rozsahu: Závažnosť 1. úrovne – kritická Produkt nie je použiteľný, čo vedie k celkovému narušeniu práce, alebo k inému závažnému dopadu na prevádzku. Reakčná doba: 1 hodina, Závažnosť 2. úrovne – vysoká Zlyhanie veľmi dôležitej čiastkovej funkčnosti produktu. Prevádzka je vážne obmedzená. Reakčná doba: 4 hodiny, Závažnosť 3. úrovne – nízka Zlyhanie menej dôležitej čiastkovej funkčnosti produktu. Produkt nefunguje podľa špecifikácií stanovených výrobcom. Prevádzka je obmedzená len čiastočne. Reakčná doba: 1 pracovný deň, Závažnosť 4. úrovne – iná Nezávažný problém. Môže to byť napr. žiadosť o dokumentáciu, všeobecnú informáciu, žiadosť o vylepšenie a pod. Reakčná doba: 2 pracovné dni.

V tabuľke nižšie sú uvedené požiadavky na softvér pre zálohovanie - požiadavky pre Backup (Kubernetes); verejný obstarávateľ požaduje uviesť cenu za minimálny pack a cenu pre **20 VM**

Technické vlastnosti	Minimálne požadované parametre
Architektúra	Riešenie musí bežať natívne v prostredí Kubernetes Namespace Riešenie musí byť plne využívať API pre podporu požiadaviek developerov Riešenie musí byť plne softvérové, nezávislé na akýchkoľvek HW platformách Riešenie nesmie vyžadovať vlastné daemon sety Riešenie nesmie mať žiadne privilegované daemonsety
Škálovateľnosť	Požadujeme dynamickú automatickú škálovateľnosť s Kubernetes Klastrom
Platforma	Riešenie musí obsahovať plnohodnotné reportovanie Riešenie musí obsahovať plnohodnotné UI Riešenie musí automaticky zálohovať Application Objects a Dependencies Riešenie musí umožniť transformácie v procese obnovy Riešenie musí umožniť automatizovaný data manažment riadený politikami Riešenie musí umožňovať automaticky priradovať politiky/pravidlá minimálne na základe TAGs, Labels, alebo názvov aplikácií Riešenie musí podporovať granulárne RPO menej než 10 min Riešenie musí podporovať failover medzi regiónmi, zónami dostupnosti, naprieč cloudmi Podpora kompresie a deduplikácie S3/NFS cieľov Riešenie musí podporovať aplikačne konzistentné, databázovo konzistentné, a crash konzistentné zálohy Požadujeme podporu polyglot persistencie
Bezpečnosť	Riešenie musí podporovať Air-Gapped Kubernetes prostredia Požadujeme podporu RBAC Riešenie musí byť plne multi-tenantné Riešenie musí poskytovať end-to-end šifrovanie Riešenie musí poskytovať immutable zálohy dát podpora OIDC alebo Tokenovej autentifikácie
Požiadavky na dodanie podpory výrobcu pre softvérový produkt	Podpora priamo od výrobcu dodávaného softvérového produktu, dĺžka podpory 3 roky od prevzatia.
	nárok na aktuálne verzie softvérového produktu, prístupné prostredníctvom portálu výrobcu,
	prístup k opravným balíkom,
	podpora poskytovaná v rozsahu 8 hodín denne v rozmedzí 9:00 – 17:00 SEČ, v pracovných dňoch,
	podpora poskytovaná telefonicky, formou emailu, alebo cez ticketovací portál výrobcu.
	prístup k dokumentácii prostredníctvom webového portálu výrobcu,
	prioritizácia riešenia nahlásených prípadov podpory podľa ich dopadu na celkovú funkčnosť softvérového produktu,
	doba odozvy pre príslušnú úroveň závažnosti musí byť garantovaná v nasledujúcom rozsahu:
	Závažnosť 1. úrovne – kritická

	Produkt nie je použiteľný, čo vedie k celkovému narušeniu práce, alebo k inému závažnému dopadu na prevádzku. Reakčná doba: 1 hodina, Závažnosť 2. úrovne – vysoká Zlyhanie veľmi dôležitej čiastkovej funkčnosti produktu. Prevádzka je vážne obmedzená. Reakčná doba: 4 hodiny, Závažnosť 3. úrovne – nízka Zlyhanie menej dôležitej čiastkovej funkčnosti produktu. Produkt nefunguje podľa špecifikácií stanovených výrobcom. Prevádzka je obmedzená len čiastočne. Reakčná doba: 1 pracovný deň, Závažnosť 4. úrovne – iná Nezávažný problém. Môže to byť napr. žiadosť o dokumentáciu, všeobecnú informáciu, žiadosť o vylepšenie a pod. Reakčná doba: 2 pracovné dni.
--	--

Verejný obstarávateľ požaduje dodanie softvérového balíka pre virtualizáciu infraštruktúry. Verejný obstarávateľ požaduje uviesť cenu podľa počtu uvedených počtov v tabuľke

Software pre virtualizáciu

Technické vlastnosti	hodnota
vSphere Ent Plus	Licencie na 20 CPU
vCenter Server Std	Jedna licencia