**OPZ – technické riešenie (cloudové služby v privátnom cloudovom riešení)**

Riešenie bude poskytované a prevádzkované v dátovom centre nachádzajúcom sa na území Slovenskej republiky určenom verejným obstarávateľom, tzn., že všetky náklady súvisiace s umiestnením riešenia v datacentre znáša verejný obstarávateľ a nemôžu byť súčasťou budúcej predloženej ponuky.

Riešenie musí podporovať multi-tenant s logickým oddelením prostredia orgán riadenia. Riešenie bude schopné podporovať funkciu, ktorá umožní orgánu riadenia vytvoriť vlastné logické členenie pre svoje podriadené organizácie v ich prostredí. Prepojenie v rámci multi-tenant bude komunikovať cez vnútornú a rýchlu sieť riešenia (backbone) a nesmie vyjsť von do internetu.

Riešenie musí umožňovať definovanie a vynucovanie politík a auditov pre multi-tenant riešenie, ktoré pomôžu zabezpečiť správne riadenie a kontrolu. Týmto sa zabezpečí efektívny governance a kontrola nad celým riešením. Riešenie musí mať vysokú mieru bezpečnosti, aby zabezpečilo ochranu dát a aplikácií pred rôznymi bezpečnostnými hrozbami a útokmi. Bezpečnostné opatrenia by mali byť dostatočne silné na to, aby zabránili neoprávnenému prístupu k dátam a chránili ich pred stratou, krádežou alebo poškodením. Zároveň by riešenie malo poskytovať základné bezpečnostné funkcie, ako sú autentifikácia, autorizácia a šifrovanie dát, aby sa minimalizoval riziko úniku dát alebo ich poškodenia. Riešenie musí umožňovať efektívne riadiť náklady pomocou odporúčaní a prognóz, ktoré pomáhajú docieliť lepšie ceny. To znamená, že musí obsahovať prehľadný dashboard, ktorý umožňuje sledovať a predikovať náklady na zdroje bežiace v cloudovom riešení. Okrem toho by malo byť možné prideliť rozpočty a stanoviť soft limit hranice, na ktoré systém automaticky upozorní pri ich prekročení. Toto všetko prispeje k efektívnejšiemu riadeniu nákladov a k lepšiemu hospodáreniu s finančnými prostriedkami.

Riešenie musí umožňovať škálovanie automaticky v určenom rozsahu. Riešenie musí podporovať operačné systémy Windows, RHEL, Suse, CentOS a Ubuntu, a zároveň musí umožniť použitie vlastného image operačného systému používateľmi. Riešenie musí umožňovať používanie procesorov od spoločností AMD a Intel a zároveň musí byť schopné podporiť použitie oboch procesorov súčasne v riešení.

Riešenie poskytuje možnosť prevádzkovania v multi-cloud prostredí (v spolupráci s lokálnymi riešeniami, VMware, hybridné cloudové riešenia, ...)

Riešenie poskytuje možnosť zdieľania virtuálnych zdrojov medzi viacerými cloudovými riešeniami v multi-cloud prostredí pripadne v reálnom verejnom cloude, zároveň umožňuje centrálnu správu takéhoto riešenia. Riešenie musí umožňovať aby tenant vedel presúval pracovné zaťaženie z riešenia do verejného cloudu, ktoré nie sú súčasťou tejto objednávky. Riešenie musí byť tiež prepojené s verejným cloudom a poskytne minimálne rovnaké technológie ako sú uvedené v tabuľke v požadovanom Sizingu.

Riešenie musí umožňovať vytvorenie softvérovo definovaného dátového centra (SDDC), ktoré bude súčasťou celého riešenia a bude komunikovať prostredníctvom vnútornej a rýchlej siete (backbone) v rámci tohto riešenia. Zároveň musí byť zabezpečené, aby SDDC nepoužívalo internetové pripojenie a všetka komunikácia prebiehala cez internú sieť riešenia. Riešenie musí byt flexibilné a škálovateľné, to znamená, že môžeme ľahko meniť a prispôsobovať riešenie podľa potreby, bez toho aby sme museli riešiť zložité a drahé zmeny infraštruktúry. Týmto požadujeme, aby riešenie disponovalo SLA (Service Level Agreement) na minimálne 99,9%. Konkrétne to znamená, že riešenie by malo byť k dispozícii takmer nepretržite, so zanedbateľným množstvom času nedostupnosti v priebehu jedného roka. Dodávateľ sa zaväzuje, že riešenie bude zabezpečené monitorovaním každej aktivity, ktorá sa týka prístupu do dátového centra a miestnosti. Každá intervencia v rámci podpory, ktorá zahŕňa vzdialený prístup dodávateľa do riešenia, bude monitorovaná a prístupy budú zaznamenané.

Riešenie bude zabezpečované dodávateľom, ktorý sa zaväzuje k poskytovaniu komplexnej podpory pre obnovu a dopĺňanie hardvéru, ako aj k poskytovaniu L1, L2 a L3 podpory na zabezpečenie manažovateľnosti, dostupnosti a výkonnosti riešenia. S cieľom zabezpečiť spoľahlivosť a neustálu prevádzku riešenia, bude dodávateľ neustále monitorovať výkonnosť a funkčnosť hardvéru a prijímať preventívne opatrenia, aby sa minimalizovali prípadné výpadky alebo poruchy. Okrem toho dodávateľ zabezpečí, že jeho podpora bude k dispozícii v prípade akejkoľvek potreby, aby sa uistil, že riešenie bude vždy dostupné a plne funkčné. Dodávateľ sa zaväzuje, že bude neustále aktualizovať a rozširovať služby riešenia, ako aj zabezpečovať ich dostupnosť počas platnosti a účinnosti zmluvy. V prípade výmeny hardvéru dodávateľ bude mať plnú zodpovednosť za všetky úkony súvisiace s výmenou, aby sa minimalizoval prípadný výpadok služieb, a objednávateľ nebude musieť zasahovať ani logisticky zabezpečovať výmenu.

Riešenie musí umožňovať nasadenie minimálne v rozsahu nasledujúcich cloudových služieb, ďalšie služby sú vítane.

Cloud služby:

* Virtuálne stroje (VM) pre operačné systémy Windows a Linux
* VMware softvérové-definované dátové centrum (SDDC)
* Kontajnery – containerd
* Registry pre kontajnery, vrátane skenovania zraniteľností
* Orchestration pomocou Kubernetes alebo OpenShift
* Serverless Computing
* DevOps nástroje, vrátane Git repozitára, Pipelines a Infrastructure-as-Code (IaC) pomocou Terraform
* Služby pre správu adresárov
* Databázové riešenia vrátane MySQL, PostgreSQL, Microsoft SQL, Oracle a Redis
* Vyhľadávanie pomocou SOLR alebo Elasticsearch
* Monitorovanie s možnosťou vytvárania upozornení, sledovania udalostí a logov
* Analytika a dashboard pre fakturáciu
* Bezpečnostné riešenia zahrňujúce správu kľúčov (HSM), šifrovanie dát a pravidlá ochrany dát
* Sieťové služby vrátane firewallu, WAF, brány aplikácií, IPS, proxy, VPN, Load Balancer, DNS a jump serverov
* Ukladanie dát – súbory, bloky, objekty a archív
* Zálohovanie súborov, databáz a archívov
* Dostupné typy diskov – HDD, SSD a NVME
* Messaging riešenia, vrátane Apache Kafka, RabbitMQ a JMS
* SIEM (Security Information and Event Management)
* Samoobslužný cloudový portál
* Nástroje pre konfiguráciu a nasadenie, ako napríklad Ansible.