# Část 1 – DR a zálohovací infrastruktura

Zadavatel v této části poptává IT infrastrukturní řešení, jehož hlavním cílem je zásadním způsobem zvýšit dostupnost a bezpečnost stávající IT infrastruktury. Prioritou je zajištění ochrany klíčových dat, minimalizace rizik spojených s kybernetickými hrozbami a udržení kontinuity provozu IT služeb i v případě výpadků či havarijních situací.

Cílem poptávaného řešení je:

* **Vybudovat záložní lokalitu** s geograficky odděleným datovým centrem pro zajištění vysoké dostupnosti a ochrany dat.
* **Posílit ochranu záloh** proti ransomware a dalším kybernetickým hrozbám prostřednictvím moderních technologií pro zálohování a pravidelnou kontrolu integrity záloh.
* **Vybudovat offline úložiště záloh** pro zajištění obnovitelnosti v případě kybernetického incidentu.

Poptávané řešení by mělo být flexibilní, jednoduše spravovatelné a zároveň finančně efektivní, aby bylo možné ho přizpůsobit konkrétním potřebám zadavatele při zachování vysoké úrovně ochrany a dostupnosti.

Požadujeme řešení, které bude zahrnovat tyto oblasti:

**Virtualizační DR cluster**  
Virtualizační cluster pro zajištění DR prostředí v záložním datovém centru. Virtualizační cluster poptáváme včetně propojovací LAN infrastruktury a souvisejících VMware licencí pro zajištění kompatibility se stávající provozovanou virtualizační platformou.

**Zálohovací a replikační řešení**  
Dodávka a implementace zálohovacího systému umožňujícího granulární obnovu dat, automatizované zálohování, šifrování, ochranu před neoprávněným přístupem a podporu nezměnitelných záloh s replikací do více lokalit. Současně by mělo řešení podporovat i možnost replikace virtuálních serverů mezi virtualizačními clustery. Zálohovací řešení poptáváme včetně příslušného HW pro běh a uložení záloh.

**Oddělený datový trezor (Vault)**  
Zajištění izolovaného úložiště pro zabezpečení záloh, s řízeným přístupem, šifrovanou replikací, nastavením retence a ochranou proti smazání či modifikaci.

Detailní požadavky jsou popsány v následujících kapitolách.

## Obecné požadavky na dodávané technologie

Níže uvádíme obecné požadavky na konfiguraci nabízeného řešení a jeho popis.

|  |  |
| --- | --- |
| **Obecné požadavky na nabízené řešení** | **Plnění požadovaných parametrů** |
|
| K prokázání skutečnosti, že nabídka odpovídá požadované kvalitě a nabízené zboží a služby jsou v souladu s požadavky Zadavatele, zahrne Dodavatel do své nabídky popis, ve kterém uvede obchodní název výrobku, rozpis hlavních komponent a detailní specifikaci rozsahu nabízených služeb tak, aby bylo možné jednoznačně určit, zda nabídka splňuje požadavky Zadavatele či nikoliv. |  |
| Deklarované funkce a technické parametry každého nabízeného zařízení musí být ověřitelné prostřednictvím oficiálních datasheetů, release notes, případně manuálů, vydaných výrobcem zařízení. Veškeré deklarované funkce, technické parametry a certifikace, musí být dostupné nejpozději dnem podání nabídky. |  |
| Veškeré nabízené zboží, i jeho části, musí být originální, nově vyrobené, nepoužité, určené pro český trh a Zadavatele. V databázi výrobce, pokud taková existuje, musí být Zadavatel veden jako první uživatel zboží. |  |
| Nabízené zboží, včetně všech interních komponent, musí jako součástí záruky zahrnovat oficiální technickou podporou výrobce tak, aby v případě závady, kterou nebude Dodavatel schopen odstranit, mohl Zadavatel tuto závadu eskalovat přímo k technické podpoře výrobce zařízení. |  |
| Nabízené zboží, včetně nabízené konfigurace interních komponent, musí splňovat požadavky ErP Lot 9 (EU 2019/424). |  |
| Výrobce ani přeprodejce žádné části řešení, včetně interních komponent, nesmí být uveden na sankčních seznamech veřejné správy České Republiky a Evropské Unie, ani nesmí být uveden ve zprávě Bezpečnostní informační služby (BIS) na seznamu rizikových entit (viz kap. 2.7 - https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2013-vz-cz.pdf) nebo ve varování Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) (viz https://nukib.gov.cz/cs/infoservis/aktuality/1303-software-i-hardware-spolecnosti-huawei-a-zte-je-bezpecnostni-hrozbou/). |  |
| Veškerý hardware požadujeme dodat z důvodu kompatibility a správy celého řešení od jednoho výrobce hardware. |  |
| Veškeré nabízené serverové komponenty musí být kompatibilní pro správu se stávajícím management SW - HPE OneView. Kompatibilita je uvedena zde: https://support.hpe.com/hpesc/public/docDisplay?docId=sd00005828en\_us&page=GUID-D7147C7F-2016-0901-066B-00000000051D.html |  |
| Nabízené řešení musí obsahovat veškerou kabeláž a SFP moduly pro zapojení jednotlivých komponent do příslušných dodávaných LAN switchů. |  |

## Virtualizační cluster

Pro zajištění dostatečného výkonu a kapacity požadujeme 11 serverů splňujících následující společné parametry:

|  |  |
| --- | --- |
| **Obecné požadavky na virtualizační cluster** | **Plnění požadovaných parametrů** |
|
| Požadovaný virtualizační cluster je složen z minimálně 11 virtualizačních serverů, které mají stejnou konfiguraci z pohledu CPU, RAM a diskové kapacity. |  |
| Požadované servery jsou kompatibilní s poptávanou virtualizační vrstvou a technologií softwarově definovaného úložiště pro vytvoření virtualizačního clusteru a umožní využití nativní replikace ze stávajícího primárního virtualizačního clusteru postaveného na VMware vSphere, vSAN a NSX technologiích. |  |
| Celková požadovaná využitelná kapacita na nabízeném clusteru (bez deduplikace a komprese) se zabezpečením proti výpadku 2 nodů a započtení provozní rezervy a režie SDS řešení je minimálně 250 TB. |  |

|  |  |  |
| --- | --- | --- |
| **Detailní parametry požadovaných virtualizačních serverů (11ks)** | | **Popis plnění požadovaných parametrů** |
|
| **Základní parametry** | 2U server určený pro montáž do standardního RACKu, duální zdroj, ližiny do racku |  |
| **Procesory (CPU)** | Požadujeme každý server osazený dvěma procesory, jejichž výkon splňuje hodnoty publikované a dohledatelné na stránkách http://www.spec.org: |  |
| V testu SPECrate2017\_int\_base(http://www.spec.org/cpu2017/results/rint2017.html) minimálně 755 bodů |  |
| V testu SPECrate2017\_fp\_base(http://www.spec.org/cpu2017/results/rfp2017.html) minimálně 1095 bodů |  |
| Procesor obsahující minimálně 24 fyzických jader. |  |
| Základní frekvence min. 4,1GHz, min. 256MB CPU Cache |  |
| **Paměť (RAM)** | 2048 GB DDR5-6400, možnost budoucího rozšíření na minimálně 3072 GB.  Ochrana paměti: Advanced ECC s multi-bit error protection, Online spare, mirrored memory a fast fault tolerance. |  |
| **Uložiště** | * 2x 480GB SSD disk v RAID 1 konfiguraci pro instalaci hypervisoru. * 7x 7,68 TB NVMe SSD disk (určený pro vSAN ESA) * Možnost osazení až 16 NVMe disků (tento požadavek neplatí pro servery osazené GPU) |  |
| **IO rozhraní (LAN)** | 4x 100GbE LAN včetně 100Gb QSFP28 SR modulů |  |
| **Integrovaná vzdálená správa** | * Server musí disponovat vyhrazeným 1Gb portem pro vzdálený management. * Management musí být konfigurovatelný pro vytváření firmware sad s možností rollback při pádu aktualizace. * Server musí podporovat bez agentový vzdálený management. Vzdálený management musí podporovat standardní webové prohlížeče pro grafickou vzdálenou konzoli spolu s tlačítkem pro Virtual Power a podporovat vzdálený boot z DVD/CD/USB zařízení a být schopen uchovávat historická data o sw upgradech a patchích. * Musí být podporována vícefaktorová autentifikace. * Musí být monitorovány změny v hw a systémové konfiguraci, musí být podporována rychlá diagnostika vzniklých problémů. * Musí být k dispozici dashboard s verzemi firmwaru a security doporučením (verze IPMI, notifikace k vícefaktorové autentifikaci aj.) |  |
| **Centrální Management serverů** | Centrální management pro správu všech nabízených serverů s následující funkcionalitou:   * Musí být umožněn rychlý pohled na spravované serverové zdroje. Minimální zobrazované položky Dashboardu jsou servery, firmware baselines, server hardware, inventory. * Systém musí být dostupný přes vlastní portál odkudkoliv. * Podporuje zobrazení centrálního panelu k rychlému posouzení celkového stavu zdraví spravovaných serverů, ke kterým má uživatel oprávnění * Oznámení o aktualizacích firmware s inteligentními aktualizacemi založenými pouze na rozdílech vůči stávajícímu stavu firmware na zařízení * Uživatelsky definovatelná firmware baseline pro skupiny serverů s podporou kontroly serverů souladu s touto baseline * Kontrola souladu se zvolenou firmware baseline může být spuštěna ručně, či automaticky * Skupinovou správu a aktualizaci firmware, kterou lze plánovat nebo spustit na vyžádání * Umožňuje spouštět aktualizaci firmware sériově a paralelně s možností zastavení při chybě * Možnost nastavení plně automatické aktualizace firmware OOB managementu při vydání nové verze * Možnost definovat šablony nastavení BIOS a lokální storage serveru * Automatická aktualizace katalogu dostupných firmware baseline výrobce * Automatické vytváření servisních incidentů pro události kritického charakteru * Možnost uživatelské konfigurace oznámení kritických incidentů pomocí notifikací v aplikaci a e-mailu pro každého uživatele * Možnost definice typů chyb pro zaslání emailové notifikace * Podpora pro připojení obrazu operačního systému (ISO) s možností připojení konfiguračního souboru pro bezobslužnou instalaci operačního systému * Omezení přístupu k jednotlivým serverům, nebo skupinám, na základě uživatelsky definovatelných rolí a politik * Jednotné místo pro auditní logy všech aktivit nástroje * Možnost exportu inventáře zvolených serverů do souboru * Zobrazení informací o konektivitě síťových portů v serveru při zapojení do podporovaných swichtů * Možnost definice a přiřazení značek ke spravovaným zařízením * Možnost filtrování a práce se zařízeními na základě přiřazených značek * Možnost zobrazení zprávy o dopadu na životní prostředí spravované infrastruktury - minimálně CO2, spotřeba a náklady na provoz pro jednotlivé servery. * Grafické uživatelské rozhraní a podpora pro automatizaci s pomocí REST API * Integrace do prostředí VMware vCenter Lifecycle Manager (vLCM) pro zjednodušení správy životního cyklu serverů přímo z konzole VMware vCenter * Bez pevného limitu množství spravovaných serverů * Server management sw musí být od stejného výrobce, jako je výrobce serveru. |  |
| **USB porty, VGA porty** | min 5 ks USB 3.2 portů (minimálně jeden zepředu, dva zadní a dva uvnitř) |  |
| min. 1 x VGA port |  |
| **Ostatní redundantní části** | ventilátory i zdroje – oboje musí být vyměnitelné za provozu,  napájecí zdroje s účinností minimálně 96% a výkonem min. 1800W každý |  |
| **Bezpečnost** | * Podpora UEFI Secure Boot a Secure Start * Funkce zabezpečení, která zajistí, že servery nespustí ohrožený kód firmwaru * Podpora FIPS 140-2 * Podpora Advanced Encryption Standard (AES) a Triple Data Encryption Standard (3DES) v prohlížeči * Podpora Commercial National Security Algorithms (CNSA) módu pro zabránění použité nezabezpečených algoritmů * Aktualizace bez neoprávněné manipulace – digitálně podepsané a ověřené komponenty * Secure Recovery – obnovení kritického firmwaru do známého dobrého stavu při detekci kompromitovaného firmwaru * Schopnost vrátit zpět starou verzi firmware * Podpora one-button secure erase * Integrovaný (nevolitelný) TPM (Trusted Platform Module) 2.0 * Podpora uzamykatelného čela serveru „Bezel Locking Kit“ * Podpora možnosti detekovat vniknutí do šasi serveru |  |
| **Kompatibilita** | Jednotlivé komponenty, zejména disky, musí být kompatibilní s VMware vSAN ESA architekturou. |  |
| **OS** | Kompatibilní s vSphere od verze 8 a vyšší, Microsoft Windows Server a Red Hat Enterprise Linux (RHEL) |  |
| **Záruka a podpora** | Součástí dodávky musí být podpora výrobce v režimu NBD onsite. |  |
| Podpora musí umožnit přístup k novým verzím FW, opravným patchům atd. |  |
| V ceně na dobu 60 měsíců. |  |

U dvou z těchto 11 virtualizačních serverů požadujeme nad rámec výše uvedených požadavků dodatečné osazení minimálně dvěma grafickými adaptéry, které jsou kompatibilní se stávající licencí NVIDIA vPC a mají minimálně 64GB paměti **(**2x grafický adaptér do každého serveru**)**, které budou sloužit pro provoz virtualizovaných desktopů v případě provozu z DR datového centra. Požadujeme grafické adaptéry kompatibilní s VMware a stávajícím HW vybavením na primární lokalitě a licencemi pro jejich virtualizaci – NVIDIA vPC.

## LAN switche

Pro zajištění konektivity jednotlivých nodů virtualizačního clusteru požadujeme 2 LAN switche. Požadovaná konfigurace je následující:

|  |  |  |
| --- | --- | --- |
| **Detailní parametry požadovaných LAN switchů (2ks)** | | **Plnění požadovaných parametrů** |
|
| **Provedení** | LAN switch rack-mountable o velikosti 1U |  |
| součástí dodávky musí být i ližiny do 19“ racku |  |
|  | Proudění vzduchu ve směru od zdrojů k I/O portům. |  |
|  | Minimálně 2x redundantní napájecí zdroje a redundantní ventilátory, hot swappable |  |
| **Konfigurace** | 32x 100G QSFP28 port |  |
|  | Minimálně 8 GB RAM. |  |
|  | Interní storage - min. 32 GB. |  |
|  | Packet Buffer min. 42 MB |  |
|  | 1GbE Management port a 1x Seriový port |  |
| **Propustnost a výkon** | Switching kapacita alespoň 6,4 Tbps. |  |
|  | Propustnost alespoň 4.76 Bpps. |  |
| **Kompatibilita** | Nabízené switche musí být podporované pro nasazení jako back-end switche pro komunikaci jednotlivých nodů v rámci navrhovaného virtualizačního clusteru. |  |
| **Napájení SAN switche** | Typ napájení: AC |  |
|  | Vstupní napětí: 230 V |  |
| **Funkcionalita** | Podpora zvýšené redundance multichassis portchannel pomocí Virtual port-channel (vPC) nebo obdobné technologie |  |
|  | Podpora standardů - 802.1D, 802.1p, 802.1Q, 802.1Qbb, 802.1Qaz, 802.1s, 802.1w, 802.3x, 802.3ad, 802.1AB |  |
|  | Podpora RDMA over Converged Ethernet (RoCEv2), Virtual routing and forwarding (VRF), OSPFv2, OSPFv3, BGPv4/v6, Equal-cost multi-path (ECMP), Policy-based routing, |  |
| **Management** | CLI  REST  Nativní management nástroje OpenSSH, SCP a FTPS  Management VRF  DHCP a v4/v6 DHCP relay |  |
| **Licence** | Dodávka musí obsahovat všechny potřebné licence pro zapojení switche v lokalitě a pro využití všech funkcí dodávaného zařízení |  |
| **Požadované SFP porty a kabely** | Ke každému LAN switchi požadujeme dodat následující příslušenství:   * 22x 100GbE QSFP28 SR * 2x 10GBE SFP+ SR * 100G QSFP28-QSFP28 DAC Cable 1m |  |
| **Záruka a podpora** | Součástí dodávky musí být podpora výrobce v režimu NBD onsite. |  |
| Podpora musí umožnit přístup k novým verzím FW, opravným patchům atd. |  |
| V ceně na dobu 60 měsíců. |  |

## VMware licence

Výše požadované HW komponenty budou použity pro běh serverové virtualizace. Vzhledem k zachování kompatibility se stávající virtualizační vrstvou kterou provozujeme v primárním datovém centru požadujeme nabídku licencí na virtualizační vrstvu VMware.

Konkrétně požadujeme nabídku na **VMware Cloud Foundation** pro minimálně **528 jader (**pokud v nabídce serverů nabízíte servery s CPU s více jak požadovanými 24 jádry požadujeme nabídku licencí navýšit na pokrytí veškerých konfigurovaných jader). Současně požadujeme pokrytí veškeré konfigurované diskové kapacity na virtualizačních serverech pomocí **VMware vSAN** licence.

Požadujeme nabídku všech výše uvedených VMware licencí na dobu 60 měsíců.

## SW pro zálohování a replikaci

Pro zajištění zabezpečení dat provozovaných systémů na virtualizačním clusteru požadujeme zálohovací SW, který bude využívat níže uvedený zálohovací HW a bude zajišťovat zálohování a případnou obnovu provozovaných systémů. Požadovaný SW bude sloužit také zejména pro zajištění možnosti ukládání záloh do oddělené infrastruktury – „datového trezoru“. Požadované parametry zálohovacího SW jsou následující:

|  |  |  |
| --- | --- | --- |
| **Detailní parametry požadovaných služeb** | | **Plnění požadovaných parametrů** |
|
| **Licence** | Licence zálohovacího SW pro zálohu celkem 530 virtuálních serverů. Licence musí umožnit využití veškeré níže uvedené funkcionality a zajistit možnost zálohovat virtuální servery jak pomocí image level zálohy, tak zároveň pomocí agentové a aplikační zálohy. |  |
| Nabízené licence nesmí omezovat velikost úložné kapacity pro zálohy ani typ a počet úložných zařízení. |  |
| Licence požadujeme s podporou/subskripcí na dobu 60 měsíců pro 230 virtuálních serverů a 12 měsíců pro 300 virtuálních serverů. |  |
| **Architektura** | Systém pro zálohování dat musí být škálovatelný přidáváním dalších komponent (např. přidáním dalšího „data moveru“ či zálohovacího úložiště) a rozšiřováním zálohovací infrastruktury. Škálovatelnost musí umožňovat rozšiřování z pohledu počtu zálohovaných klientů různého typu i objemu uložených dat. |  |
| Zálohovací software je nezávislý na hardware pro instalaci komponent zálohovací infrastruktury (backup server, „data mover“, proxy server a další. Požadovaná funkcionalita zálohovacího řešení nesmí být vázána na konkrétní typ serveru či úložného zařízení. |
| Software umožňuje podporu široké škály různých typů zálohovacích úložišť jako například – Diskové blokové nebo souborové úložiště, objektové úložiště on-premise nebo v cloudu, archivní cloudová úložiště a pásková úložiště včetně managementu páskových médií. |
| Řešení umožňuje šifrovat komunikaci mezi jednotlivými komponentami zálohovacího systému (HTTPS/SSL apod.) |
| **Záloha virtuálních serverů** | Software podporuje bezagentové image zálohování virtuálních serverů na platformách VMware, Microsoft Hyper-V, Proxmox, OpenStack, RHEV, Microsoft Azure a AWS. |  |
| Software umožňuje provádět zálohu modifikovaných bloků (CBT) virtuálních serverů na platformách VMware, Hyper-V, Microsoft Azure, Openstack. |
| Pro virtuální prostředí VMware, Microsoft Hyper-V, OpenStack a Microsoft Azure umožňuje software provádět bezagentové aplikačně konzistentní zálohy aplikací Active Directory, Microsoft SQL, MS Exchange, MS Sharepoint, Oracle for Windows, MySQL (včetně záloh a odmazávání transakčních logů). Software dále umožňuje provést point-in-time obnovu takto odzálohovaných aplikací/databází pomocí agenta bez nutnosti obnovy celého virt. serveru. |
| Software umožňuje obnovu image zálohy virt. serveru do původního nebo jiného umístění. Software dále umožňuje obnovu jenotlivých souborů souborů z virt. serveru na virtuální či fyzický server. |
| Software umožňuje obnovu image zálohy virtuálního stroje VMware s okamžitým spuštěním obnovovaného stroje z diskového úložiště záloh (live restore). |
| Software umožňuje obnovu image zálohy virtuálního serveru VMware přímo do prostředí Microsoft Hyper-V, Microsoft Azure, OpenStack. |
| Software umožňuje obnovu zálohy image zálohy virtuálního serveru Hyper-V přímo do prostředí Amazon, Microsoft Azure. |
| Software umožňuje obnovu serverů s operačním systémem Linux/Windows z fyzického serveru přímo do vitruálního prostředí VMware či Hyper-V. |
| **Záloha databází** | Software zahrnuje aplikační agenty pro online zálohování databází/aplikací MS SQL Server, Oracle, MySQL, PostgreSQL, MongoDB. |  |
| Software umožňuje nastavit automatické zálohování transakčních logů databází dle následujících kritérií: 1) minimální časový interval mezi zálohami logů; 2) minimální procentuální obsazení disku s trans. logy; 3) pevný interval mezi zálohami logů. |
| Software umožňuje provádět obnovu s granularitou na úroveň tabulky pro databáze MS SQL, Oracle a PostgreSQL. |
| Je požadováno, aby řešení umožňovalo automatické spuštění zálohování databázových logů při splnění stanovených kritérií – například spuštění zálohy v okamžiku, kdy se cílové úložiště pro archivní logy zaplní na definovanou kapacitu. |  |
| Je požadováno, aby řešení podporovalo automatické vyhledávání SQL instancí na fyzických i virtuálních serverech. |  |
| **Kubernetes** | Je požadováno, aby řešení umožňovalo zálohovat, obnovovat a migrovat stavové Kubernetes aplikace a data. |  |
| Je požadováno, aby řešení automaticky vyhledávalo a chránilo objekty pomocí labelů, selektorů nebo jmenných prostorů (namespaces). |  |
| Je požadováno, aby řešení umožňovalo zálohování jakéhokoliv Kubernetes clusteru – on-premise nebo v cloudu (například GCP, AWS), včetně spravovaných Kubernetes PaaS služeb (Google Kubernetes Engine, Amazon EKS, Azure AKS). |  |
| Je požadováno, aby řešení umožňovalo zálohovat Kubernetes aplikace, přičemž aplikací může být pod, deployment, StatefulSet nebo workload. |  |
| Je požadováno, aby řešení umožňovalo zálohovat persistentní svazky a PersistentVolumeClaim (PVC). |  |
| Je požadováno, aby řešení umožňovalo zálohovat definice vlastních zdrojů (Custom Resource Definitions – CRDs). |  |
| Je požadováno, aby řešení umožňovalo obnovit kompletní aplikaci do předchozího bodu v čase, včetně automatického nasazení jako nové aplikace nebo do nového clusteru. |  |
| Je požadováno, aby řešení umožňovalo obnovit individuální datový svazek z aplikace a připojit jej k nové aplikaci. |  |
| Je požadováno, aby řešení umožňovalo obnovit nebo stáhnout soubory a složky z datových svazků nebo z aplikačních YAML manifestů. |  |
| Je požadováno, aby řešení umožňovalo obnovu na úrovni aplikace/dat, datových svazků a souborů/složek v rámci svazku. |  |
| Je požadováno, aby řešení umožňovalo obnovit do aktuálního nebo jiného svazku, aplikace či clusteru (in-place / out-of-place). |  |
| Je požadováno, aby řešení podporovalo CNCF certifikované Kubernetes distribuce a ovladače Cloud Storage Interface (CSI). |  |
| **Podpora Public Cloud** | Software umožňuje ukládat záložní/archivní data na diskovém úložišti, páskovém úložišti nebo na úložišti v public cloudu. Software umožňuje přímý zápis dat alespoň do násl. cloudových úložišť: Amazon Glacier, Amazon S3, Google, Microsoft Azure Storage, OpenStack Object Storage, Oracle Cloud Storage Archive Service. |  |
| Pro seeding záložních dat na cloudovém úložišti Amazon AWS S3 je možné využít AWS Snowball. |
| Software poskytuje přímou konektivitu do podporovaných cloudových úložišť bez nutnosti použít gateway komponentu. |
| Software umožňuje specializovaným agentem zálohování dat aplikací Microsoft Office 365 (MS Exchange Online, MS Sharepoint Online, MS OneDrive). |
| Software umožňuje pomocí agenta pro MS SQL zálohování dat Azure SQL databází. Obnovu databáze Azure SQL lze provést i do on-premise MS SQL serveru. |
| Software umožňuje pomocí agenta pro MS SQL obnovu SQL databáze z on-premise do Azure SQL. |
| **Pokročilá funkcionalita** | Software umožňuje zálohovat Virtuální servery na VMware a Hyper-V platformě a databáze MS SQL, Oracle, MySQL a PostgreSQL pomocí aplikačně konzistentních snapshotů na podporovaných diskových systémech. Konfiguraci těchto záloh lze provádět prostřednictvím grafického rozhraní administrační konzole. |  |
| Software umožňuje ukládání/replikaci vytvořených hardwarových snapshotů do deduplikovaného diskového úložiště zálohovacího systému. |
| **Deduplikace** | Software umožňuje provádět softwarovou deduplikaci dat na zdroji (klientu zál. systému) nebo na serveru zálohovacího systému. |  |
| Deduplikační funkce zálohovacího software jsou nezávislé na použitém hardware úložiště dat. Jako úložiště deduplikovaných dat lze využít diskovou storage jakéhokoliv vendora s odpovídající konektivitou, výkonem a kapacitou nebo i server s interní diskovou kapacitou. |  |
| Software umožňuje ukládání softwarově deduplikovaných dat na diskovém úložišti nebo na úložišti v public cloudu. |  |
| Software umožňuje provádět softwarovou deduplikaci dat všech klientů vůči datům všech ostatních klientů. Softwarová deduplikace není omezena na data jenotlivých jobů, klientů či agentů. |  |
| Software umožňuje nastavit replikaci deduplikovaných dat mezi datovými centry bez nutnosti rehydratace dat. |  |
| **Bezpečnost** | Software zajišťuje automatickou detekci ransomware útoků na klientech zálohovaných agentem. |  |
| Software zajišťuje ochranu diskových úložišť záloh před útoky ransomware. |  |
| Je požadováno, aby řešení automaticky monitorovalo chování souborů a detekovalo podezřelé aktivity charakteristické pro ransomware (např. hromadné šifrování souborů, nestandardní změny dat). |  |
| Je požadováno, aby řešení umožňovalo automatické označení a karanténu záloh, u kterých byla detekována možná infekce ransomwarem, a zabránilo jejich použití k obnově bez následného prověření. |  |
| Je požadováno, aby řešení podporovalo integraci s dalšími bezpečnostními systémy (např. SIEM) za účelem předávání informací o detekovaných incidentech. |  |
| Je požadováno, aby řešení umožňovalo obnovu dat z nezasažených (nemodifikovaných) záloh v případě útoku ransomwarem. |  |
| **Zálohování** | Software umožňuje nastavit softwarové omezení využití šířky pásma na datovém spoji mezi servery a klienty zálohovacího systému. Omezení využití šířky pásma lze prostředky zálohovacího systému naplánovat na jednotlivé dny/hodiny. |  |
| **Replikace** | Software umožňuje replikovat VMware virtuální servery mezi dvěma VMware clustery pomocí kontinuální replikace nevyužívající VMware snapshoty. |  |
| **Management** | Software je možné spravovat z grafické HTML 5 konzole s podporou kompletní požadované funkcionality. |  |
| Software využívá RBAC (Role-Based Access Control) pro autorizaci uživatelů k veškerým administračním či uživatelským činnostem v zálohovacím systému. |  |
| Software umožňuje integraci se systémem CyberARC pro uložení požadovaných přístupových oprávnění k zálohovaným systémům. |  |
| Software umožňuje nastavení uživatelských kvót k omezení objemu záložních dat pro jednotlivé uživatele. Kvótu pro jednotlivé uživatele je možné nastavit na úrovni skupiny, do které jsou uživatelé zařazeni. |  |
| Software umožňuje provádět centrální administraci včetně úloh zálohování a obnovy pomocí příkazové řádky. |  |
| Software umožňuje napojení administračních rozhraní třetích stran pomocí rozhraní REST API. |  |
| Všechny funkce zálohování, obnovy dat či archivace dat musí být přístupné z jednotné centrální administrační konzole s grafickým uživatelským rozhraním. |  |
| Software poskytuje multi-uživatelské prostředí s možností definovat různá oprávnění a role. Software dále umožňuje autentizaci uživatelů a skupin přes Windows Active Directory (LDAP) včetně možnosti Single Sign On (SSO) autentizace k administrační konzoli zálohovacího systému. |  |
| Software podporuje multifaktorovou autentizaci uživatelů. |  |
| Software podporuje schvalování vybraných operací více administrátory. |  |
| Software umožňuje vytvoření dynamických skupin klientů, do kterých jsou klienti automaticky zařazeny na základě splnění určitých kritérií (např. typ nainstalovaného agenta na klientu, klient offline po určitou min. dobu, verze klienta, typ a verze OS). Autorizace správy skupiny klientů může být namapována na skupiny administrátorů. |  |
| Software umožňuje nastavit notifikaci definovaných událostí v zálohovacím systému pomocí e-mailů, SNMP trapů, Windows Event Vieweru, RSS feedů a SCOM alertů. |  |
| Software umožňuje instalaci grafické administrační konzole na OS Windows, Linux, MacOS. |  |
| Software zajišťuje žurnálování změn v konfiguraci zálohovacího systému. |  |
| Software umožňuje provádět autentizaci uživatelů s využitím externích adresářových služeb. Podporovány jsou alespoň následující adr. služby: MS Active Directory, Apple Directory, Domino Directory Service, JumpCloud Directory, RADIUS, Oracle Directory Service. |  |
| Software umožňuje "push" instalaci a upgrade agentů na klientech bez nutnosti vzdálené konzole (RDP) ke klientům. Software také umožňuje provést jakoukoliv konfigurační změnu agentů na klientech z centrální grafické administrační konzole. |  |
| **Obecné** |  |  |
| Software podporuje replikaci zálohovaných dat mezi diskovým, páskovým a cloudovým úložištěm (v jakékoliv kombinaci). |  |
| Software umožňuje replikaci dat několika "zálohovacích politik" na jednu pásku. |  |
| Software umožňuje jednoduché rozšíření úložiště záloh přidáním datové cesty do již existujícího poolu nebo navýšením kapacity existující datové cesty.  Software umožňuje instalaci řídících komponent, zejména pak řídícího zálohovacího serveru na Windows Server i Linux OS se zachováním veškeré požadované funkcionality. |  |

## HW pro zálohování

Pro zajištění uložení záloh v rámci datových center požadujeme níže specifikovaný management zálohovací server a storage servery určené pro instalaci komponent nabízeného zálohovacího serveru. Jednotlivé servery musí splňovat následující parametry:

### Zálohovací server

|  |  |  |
| --- | --- | --- |
| **Detailní parametry požadovaného backup serveru (1ks)** | | **Plnění požadovaných parametrů** |
|
| **Základní parametry** | 1U server určený pro montáž do standardního RACKu, duální zdroj, ližiny do racku |  |
| **Procesory (CPU)** | Požadujeme server osazený jedním procesorem. |  |
| Jeden procesor obsahující minimálně 16 fyzických jader. |  |
| Základní frekvence min. 2,0GHz |  |
| **Paměť (RAM)** | 128 GB DDR5, možnost budoucího rozšíření minimálně na dvojnásobek. |  |
| **Diskový Řadič** | RAID diskový řadič s podporou minimálně RAID 0,1 a 5 |  |
| **Uložiště** | * 2x 480 GB disk v RAID 1 konfiguraci pro instalaci OS * 2x 960 GB SSD disk v RAID 1 konfiguraci |  |
| **IO rozhraní (LAN/SAN)** | 2x 10/25GbE LAN |  |
| **Integrovaná vzdálená správa** | * Server musí disponovat vyhrazeným 1Gb portem pro vzdálený management. * Management musí být konfigurovatelný pro vytváření firmware sad s možností rollback při pádu aktualizace. * Server musí podporovat bez agentový vzdálený management. Vzdálený management musí podporovat standardní webové prohlížeče pro grafickou vzdálenou konzoli spolu s tlačítkem pro Virtual Power a podporovat vzdálený boot z DVD/CD/USB zařízení a být schopen uchovávat historická data o sw upgradech a patchích. * Musí být podporována vícefaktorová autentifikace. * Musí být monitorovány změny v hw a systémové konfiguraci, musí být podporována rychlá diagnostika vzniklých problémů. * Musí být k dispozici dashboard s verzemi firmwaru a security doporučením (verze IPMI, notifikace k vicefaktorové autentifikaci aj.) |  |
| **USB porty, VGA porty** | min 3 ks USB 3.0 portů (minimálně jeden zepředu a dva zadní). |  |
| min. 1 x VGA port |  |
| **Ostatní redundantní části** | ventilátory i zdroje – oboje musí být vyměnitelné za provozu,  napájecí zdroje s účinností minimálně 96% a výkonem min. 1000W každý |  |
| **Bezpečnost** | * Podpora UEFI Secure Boot a Secure Start * Funkce zabezpečení, která zajistí, že servery nespustí ohrožený kód firmwaru * Podpora FIPS 140-2 * Podpora Advanced Encryption Standard (AES) a Triple Data Encryption Standard (3DES) v prohlížeči * Podpora Commercial National Security Algorithms (CNSA) módu pro zabránění použité nezabezpečených algoritmů * Aktualizace bez neoprávněné manipulace – digitálně podepsané a ověřené komponenty * Secure Recovery – obnovení kritického firmwaru do známého dobrého stavu při detekci kompromitovaného firmwaru * Schopnost vrátit zpět starou verzi firmware * Podpora one-button secure erase * Integrovaný (nevolitelný) TPM (Trusted Platform Module) 2.0 * Podpora uzamykatelného čela serveru „Bezel Locking Kit“ * Podpora možnosti detekovat vniknutí do šasi serveru |  |
| **Záruka a podpora** | Součástí dodávky musí být podpora výrobce v režimu NBD onsite. |  |
| Podpora musí umožnit přístup k novým verzím FW, opravným patchům atd. |  |
| V ceně na dobu 60 měsíců. |  |
| **Požadovaná funkcionalita ve spolupráci s nabízeným zálohovacím SW** | | |
| Je požadováno, aby navržená konfigurace byla plně kompatibilní se zálohovacím softwarem pro možnost instalace a běhu centrální řídící komponenty nabízeného zálohovacího řešení. | |  |
| Na nabízeném serveru je možné instalovat jak Windows Server, tak Linux OS včetně podpory těchto OS ze strany nabízeného zálohovacího systému pro instalaci centrální management komponenty. | |  |

### Storage servery

|  |  |  |
| --- | --- | --- |
| **Detailní parametry požadovaného storage serveru (2ks)** | | **Plnění požadovaných parametrů** |
|
| **Základní parametry** | 2U server určený pro montáž do standardního RACKu, duální zdroj, ližiny do racku |  |
| **Procesory (CPU)** | Požadujeme každý server osazený dvěma procesory. |  |
| Dva procesory, každý obsahující minimálně 16 fyzických jader. |  |
| Základní frekvence min. 2,0GHz |  |
| **Paměť (RAM)** | 256 GB DDR5, možnost budoucího rozšíření minimálně na dvojnásobek. |  |
| **Diskový Řadič** | RAID diskový řadič s podporou minimálně RAID 0,1,5 a 6 |  |
| **Uložiště** | * 2x 480 GB NVMe disk v RAID 1 konfiguraci pro instalaci OS * 2x 6.4 TB SSD (3 DWPD) * 24x SAS HDD 20TB |  |
| **IO rozhraní (LAN/SAN)** | 4x 10/25GbE LAN |  |
| **Integrovaná vzdálená správa** | * Server musí disponovat vyhrazeným 1Gb portem pro vzdálený management. * Management musí být konfigurovatelný pro vytváření firmware sad s možností rollback při pádu aktualizace. * Server musí podporovat bez agentový vzdálený management. Vzdálený management musí podporovat standardní webové prohlížeče pro grafickou vzdálenou konzoli spolu s tlačítkem pro Virtual Power a podporovat vzdálený boot z DVD/CD/USB zařízení a být schopen uchovávat historická data o sw upgradech a patchích. * Musí být podporována vícefaktorová autentifikace. * Musí být monitorovány změny v hw a systémové konfiguraci, musí být podporována rychlá diagnostika vzniklých problémů. * Musí být k dispozici dashboard s verzemi firmwaru a security doporučením (verze IPMI, notifikace k vicefaktorové autentifikaci aj.) |  |
| **Centrální Management serverů** | Centrální management pro správu všech nabízených serverů s následující funkcionalitou:   * Musí být umožněn rychlý pohled na spravované serverové zdroje. Minimální zobrazované položky Dashboardu jsou servery, firmware baselines, server hardware, inventory. * Systém musí být dostupný přes vlastní portál odkudkoliv. * Podporuje zobrazení centrálního panelu k rychlému posouzení celkového stavu zdraví spravovaných serverů, ke kterým má uživatel oprávnění * Oznámení o aktualizacích firmware s inteligentními aktualizacemi založenými pouze na rozdílech vůči stávajícímu stavu firmware na zařízení * Uživatelsky definovatelná firmware baseline pro skupiny serverů s podporou kontroly serverů souladu s touto baseline * Kontrola souladu se zvolenou firmware baseline může být spuštěna ručně, či automaticky * Skupinovou správu a aktualizaci firmware, kterou lze plánovat nebo spustit na vyžádání * Umožňuje spouštět aktualizaci firmware sériově a paralelně s možností zastavení při chybě * Možnost nastavení plně automatické aktualizace firmware OOB managementu při vydání nové verze * Možnost definovat šablony nastavení BIOS a lokální storage serveru * Automatická aktualizace katalogu dostupných firmware baseline výrobce * Automatické vytváření servisních incidentů pro události kritického charakteru * Možnost uživatelské konfigurace oznámení kritických incidentů pomocí notifikací v aplikaci a e-mailu pro každého uživatele * Možnost definice typů chyb pro zaslání emailové notifikace * Podpora pro připojení obrazu operačního systému (ISO) s možností připojení konfiguračního souboru pro bezobslužnou instalaci operačního systému * Omezení přístupu k jednotlivým serverům, nebo skupinám, na základě uživatelsky definovatelných rolí a politik * Jednotné místo pro auditní logy všech aktivit nástroje * Možnost exportu inventáře zvolených serverů do souboru * Zobrazení informací o konektivitě síťových portů v serveru při zapojení do podporovaných switchů * Možnost definice a přiřazení značek ke spravovaným zařízením * Možnost filtrování a práce se zařízeními na základě přiřazených značek * Možnost zobrazení zprávy o dopadu na životní prostředí spravované infrastruktury - minimálně CO2, spotřeba a náklady na provoz pro jednotlivé servery. * Grafické uživatelské rozhraní a podpora pro automatizaci s pomocí REST API * Bez pevného limitu množství spravovaných serverů * Server management sw musí být od stejného výrobce, jako je výrobce serveru. |  |
| **USB porty, VGA porty** | min 4 ks USB 3.0 portů (minimálně jeden zepředu a dva zadní). |  |
| min. 1 x VGA port |  |
| **Ostatní redundantní části** | ventilátory i zdroje – oboje musí být vyměnitelné za provozu,  napájecí zdroje s účinností minimálně 96% a výkonem min. 1000W každý |  |
| **Bezpečnost** | * Podpora UEFI Secure Boot a Secure Start * Funkce zabezpečení, která zajistí, že servery nespustí ohrožený kód firmwaru * Podpora FIPS 140-2 * Podpora Advanced Encryption Standard (AES) a Triple Data Encryption Standard (3DES) v prohlížeči * Podpora Commercial National Security Algorithms (CNSA) módu pro zabránění použité nezabezpečených algoritmů * Aktualizace bez neoprávněné manipulace – digitálně podepsané a ověřené komponenty * Secure Recovery – obnovení kritického firmwaru do známého dobrého stavu při detekci kompromitovaného firmwaru * Schopnost vrátit zpět starou verzi firmware * Podpora one-button secure erase * Integrovaný (nevolitelný) TPM (Trusted Platform Module) 2.0 * Podpora uzamykatelného čela serveru „Bezel Locking Kit“ * Podpora možnosti detekovat vniknutí do šasi serveru |  |
| **OS** | Bez operačního systému. |  |
| **Záruka a podpora** | Součástí dodávky musí být podpora výrobce v režimu NBD onsite. |  |
| Podpora musí umožnit přístup k novým verzím FW, opravným patchům atd. |  |
| V ceně na dobu 60 měsíců. |  |
| **Požadovaná funkcionalita ve spolupráci s nabízeným zálohovacím SW** | | |
| Je požadováno, aby navržená konfigurace byla plně kompatibilní se zálohovacím softwarem pro možnost plného využití konfigurované kapacity s možností zajištění deduplikace ukládaných záloh pro celou konfigurovanou kapacitu. | |  |
| Na nabízeném serveru je možné instalovat komponenty nabízeného zálohovacího software pro zajištění zálohování virtualizace | |  |
| Na nabízeném serveru je možné instalovat jak Windows Server, tak Linux OS včetně podpory těchto OS ze strany nabízeného zálohovacího systému (včetně splnění výše uvedených podmínek). | |  |
| Konfiguraci bude možné v budoucnu doplnit o konektivitu pro připojení páskové mechaniky a zajistit tak možnost duplikace záloh na pásková média. | |  |

## HW pro zálohování – oddělený datový trezor

Pro zajištění obnovitelnosti záloh i v případě rozsáhlejšího kybernetického útoku a kompromitaci primárního prostředí požadujeme nabídku na infrastrukturu, která bude tvořit oddělený datový trezor pro kopie záloh. Požadujeme následující technologie:

### Zálohovací server

|  |  |  |
| --- | --- | --- |
| **Detailní parametry požadovaného zálohovacího serveru (1ks)** | | **Plnění požadovaných parametrů** |
|
| **Základní parametry** | 1U server určený pro montáž do standardního RACKu, duální zdroj, ližiny do racku |  |
| **Procesory (CPU)** | Požadujeme server osazený jedním procesorem. |  |
| Jeden procesor obsahující minimálně 16 fyzických jader. |  |
| Základní frekvence min. 2,0GHz. |  |
| **Paměť (RAM)** | 128 GB DDR5, možnost budoucího rozšíření na dvojnásobek. |  |
| **Diskový Řadič** | RAID řadič s podporou alespoň RAID 0/1/1+0 |  |
| **Uložiště** | * 2x 480GB SSD disk v RAID 1 konfiguraci pro instalaci OS * 2x 960 SSD disk v RAID 1 konfiguraci |  |
| **IO rozhraní (LAN/SAN)** | 2x 10/25GbE LAN  4x 1Gbit LAN |  |
| **Integrovaná vzdálená správa** | * Server musí disponovat vyhrazeným 1Gb portem pro vzdálený management. * Management musí být konfigurovatelný pro vytváření firmware sad s možností rollback při pádu aktualizace. * Server musí podporovat bez agentový vzdálený management. Vzdálený management musí podporovat standardní webové prohlížeče pro grafickou vzdálenou konzoli spolu s tlačítkem pro Virtual Power a podporovat vzdálený boot z DVD/CD/USB zařízení a být schopen uchovávat historická data o sw upgradech a patchích. * Musí být podporována vícefaktorová autentifikace. * Musí být monitorovány změny v hw a systémové konfiguraci, musí být podporována rychlá diagnostika vzniklých problémů. * Musí být k dispozici dashboard s verzemi firmwaru a security doporučením (verze IPMI, notifikace k vicefaktorové autentifikaci aj.) |  |
| **Centrální Management serverů** | Centrální management pro správu všech nabízených serverů s následující funkcionalitou:   * Musí být umožněn rychlý pohled na spravované serverové zdroje. Minimální zobrazované položky Dashboardu jsou servery, firmware baselines, server hardware, inventory. * Systém musí být dostupný přes vlastní portál odkudkoliv. * Podporuje zobrazení centrálního panelu k rychlému posouzení celkového stavu zdraví spravovaných serverů, ke kterým má uživatel oprávnění * Oznámení o aktualizacích firmware s inteligentními aktualizacemi založenými pouze na rozdílech vůči stávajícímu stavu firmware na zařízení * Uživatelsky definovatelná firmware baseline pro skupiny serverů s podporou kontroly serverů souladu s touto baseline * Kontrola souladu se zvolenou firmware baseline může být spuštěna ručně, či automaticky * Skupinovou správu a aktualizaci firmware, kterou lze plánovat nebo spustit na vyžádání * Umožňuje spouštět aktualizaci firmware sériově a paralelně s možností zastavení při chybě * Možnost nastavení plně automatické aktualizace firmware OOB managementu při vydání nové verze * Možnost definovat šablony nastavení BIOS a lokální storage serveru * Automatická aktualizace katalogu dostupných firmware baseline výrobce * Automatické vytváření servisních incidentů pro události kritického charakteru * Možnost uživatelské konfigurace oznámení kritických incidentů pomocí notifikací v aplikaci a e-mailu pro každého uživatele * Možnost definice typů chyb pro zaslání emailové notifikace * Podpora pro připojení obrazu operačního systému (ISO) s možností připojení konfiguračního souboru pro bezobslužnou instalaci operačního systému * Omezení přístupu k jednotlivým serverům, nebo skupinám, na základě uživatelsky definovatelných rolí a politik * Jednotné místo pro auditní logy všech aktivit nástroje * Možnost exportu inventáře zvolených serverů do souboru * Zobrazení informací o konektivitě síťových portů v serveru při zapojení do podporovaných switchů * Možnost definice a přiřazení značek ke spravovaným zařízením * Možnost filtrování a práce se zařízeními na základě přiřazených značek * Možnost zobrazení zprávy o dopadu na životní prostředí spravované infrastruktury – minimálně CO2, spotřeba a náklady na provoz pro jednotlivé servery. * Grafické uživatelské rozhraní a podpora pro automatizaci s pomocí REST API * Bez pevného limitu množství spravovaných serverů * Server management sw musí být od stejného výrobce, jako je výrobce serveru. |  |
| **USB porty, VGA porty** | min 3 ks USB 3.0 portů (minimálně jeden zepředu a dva zadní). |  |
| min. 1 x VGA port |  |
| **Ostatní redundantní části** | ventilátory i zdroje – oboje musí být vyměnitelné za provozu,  napájecí zdroje s účinností minimálně 96% a výkonem min. 1000W každý |  |
| **Bezpečnost** | * Podpora UEFI Secure Boot a Secure Start * Funkce zabezpečení, která zajistí, že servery nespustí ohrožený kód firmwaru * Podpora FIPS 140-2 * Podpora Advanced Encryption Standard (AES) a Triple Data Encryption Standard (3DES) v prohlížeči * Podpora Commercial National Security Algorithms (CNSA) módu pro zabránění použité nezabezpečených algoritmů * Aktualizace bez neoprávněné manipulace – digitálně podepsané a ověřené komponenty * Secure Recovery – obnovení kritického firmwaru do známého dobrého stavu při detekci kompromitovaného firmwaru * Schopnost vrátit zpět starou verzi firmware * Podpora one-button secure erase * Integrovaný (nevolitelný) TPM (Trusted Platform Module) 2.0 * Podpora uzamykatelného čela serveru „Bezel Locking Kit“ * Podpora možnosti detekovat vniknutí do šasi serveru |  |
| **OS** | Bez operačního systému. |  |
| **Záruka a podpora** | Součástí dodávky musí být podpora výrobce v režimu NBD onsite. |  |
| Podpora musí umožnit přístup k novým verzím FW, opravným patchům atd. |  |
| V ceně na dobu 60 měsíců. |  |
| **Požadovaná funkcionalita ve spolupráci s nabízeným zálohovacím SW** | | |
| Je požadováno, aby navržená konfigurace byla plně kompatibilní se zálohovacím softwarem pro možnost instalace a běhu centrální řídící komponenty nabízeného zálohovacího řešení. | |  |
| Na nabízeném serveru je možné instalovat jak Windows Server, tak Linux OS včetně podpory těchto OS ze strany nabízeného zálohovacího systému pro instalaci centrální management komponenty. | |  |

### Storage server

|  |  |  |
| --- | --- | --- |
| **Detailní parametry požadovaného storage serveru (1ks)** | | **Plnění požadovaných parametrů** |
|
| **Základní parametry** | 2U server určený pro montáž do standardního RACKu, duální zdroj, ližiny do racku |  |
| **Procesory (CPU)** | Požadujeme každý server osazený dvěma procesory. |  |
| Dva procesory, každý obsahující minimálně 16 fyzických jader. |  |
| Základní frekvence min. 2,0GHz |  |
| **Paměť (RAM)** | 256 GB DDR5, možnost budoucího rozšíření minimálně na dvojnásobek. |  |
| **Diskový Řadič** | RAID diskový řadič s podporou minimálně RAID 0,1,5 a 6 |  |
| **Uložiště** | * 2x 480 GB NVMe disk v RAID 1 konfiguraci pro instalaci OS * 2x NVMe 6.4 TB (3 DWPD) * 24x SAS HDD 20TB |  |
| **IO rozhraní (LAN/SAN)** | 4x 10/25GbE LAN |  |
| **Integrovaná vzdálená správa** | * Server musí disponovat vyhrazeným 1Gb portem pro vzdálený management. * Management musí být konfigurovatelný pro vytváření firmware sad s možností rollback při pádu aktualizace. * Server musí podporovat bez agentový vzdálený management. Vzdálený management musí podporovat standardní webové prohlížeče pro grafickou vzdálenou konzoli spolu s tlačítkem pro Virtual Power a podporovat vzdálený boot z DVD/CD/USB zařízení a být schopen uchovávat historická data o sw upgradech a patchích. * Musí být podporována vícefaktorová autentifikace. * Musí být monitorovány změny v hw a systémové konfiguraci, musí být podporována rychlá diagnostika vzniklých problémů. * Musí být k dispozici dashboard s verzemi firmwaru a security doporučením (verze IPMI, notifikace k vicefaktorové autentifikaci aj.) |  |
| **Centrální Management serverů** | Centrální management pro správu všech nabízených serverů s následující funkcionalitou:   * Musí být umožněn rychlý pohled na spravované serverové zdroje. Minimální zobrazované položky Dashboardu jsou servery, firmware baselines, server hardware, inventory. * Systém musí být dostupný přes vlastní portál odkudkoliv. * Podporuje zobrazení centrálního panelu k rychlému posouzení celkového stavu zdraví spravovaných serverů, ke kterým má uživatel oprávnění * Oznámení o aktualizacích firmware s inteligentními aktualizacemi založenými pouze na rozdílech vůči stávajícímu stavu firmware na zařízení * Uživatelsky definovatelná firmware baseline pro skupiny serverů s podporou kontroly serverů souladu s touto baseline * Kontrola souladu se zvolenou firmware baseline může být spuštěna ručně, či automaticky * Skupinovou správu a aktualizaci firmware, kterou lze plánovat nebo spustit na vyžádání * Umožňuje spouštět aktualizaci firmware sériově a paralelně s možností zastavení při chybě * Možnost nastavení plně automatické aktualizace firmware OOB managementu při vydání nové verze * Možnost definovat šablony nastavení BIOS a lokální storage serveru * Automatická aktualizace katalogu dostupných firmware baseline výrobce * Automatické vytváření servisních incidentů pro události kritického charakteru * Možnost uživatelské konfigurace oznámení kritických incidentů pomocí notifikací v aplikaci a e-mailu pro každého uživatele * Možnost definice typů chyb pro zaslání emailové notifikace * Podpora pro připojení obrazu operačního systému (ISO) s možností připojení konfiguračního souboru pro bezobslužnou instalaci operačního systému * Omezení přístupu k jednotlivým serverům, nebo skupinám, na základě uživatelsky definovatelných rolí a politik * Jednotné místo pro auditní logy všech aktivit nástroje * Možnost exportu inventáře zvolených serverů do souboru * Zobrazení informací o konektivitě síťových portů v serveru při zapojení do podporovaných switchů * Možnost definice a přiřazení značek ke spravovaným zařízením * Možnost filtrování a práce se zařízeními na základě přiřazených značek * Možnost zobrazení zprávy o dopadu na životní prostředí spravované infrastruktury - minimálně CO2, spotřeba a náklady na provoz pro jednotlivé servery. * Grafické uživatelské rozhraní a podpora pro automatizaci s pomocí REST API * Bez pevného limitu množství spravovaných serverů * Server management sw musí být od stejného výrobce, jako je výrobce serveru. |  |
| **USB porty, VGA porty** | min 4 ks USB 3.0 portů (minimálně jeden zepředu a dva zadní). |  |
| min. 1 x VGA port |  |
| **Ostatní redundantní části** | ventilátory i zdroje – oboje musí být vyměnitelné za provozu,  napájecí zdroje s účinností minimálně 96% a výkonem min. 1000W každý |  |
| **Bezpečnost** | * Podpora UEFI Secure Boot a Secure Start * Funkce zabezpečení, která zajistí, že servery nespustí ohrožený kód firmwaru * Podpora FIPS 140-2 * Podpora Advanced Encryption Standard (AES) a Triple Data Encryption Standard (3DES) v prohlížeči * Podpora Commercial National Security Algorithms (CNSA) módu pro zabránění použité nezabezpečených algoritmů * Aktualizace bez neoprávněné manipulace – digitálně podepsané a ověřené komponenty * Secure Recovery – obnovení kritického firmwaru do známého dobrého stavu při detekci kompromitovaného firmwaru * Schopnost vrátit zpět starou verzi firmware * Podpora one-button secure erase * Integrovaný (nevolitelný) TPM (Trusted Platform Module) 2.0 * Podpora uzamykatelného čela serveru „Bezel Locking Kit“ * Podpora možnosti detekovat vniknutí do šasi serveru |  |
| **OS** | Bez operačního systému. |  |
| **Záruka a podpora** | Součástí dodávky musí být podpora výrobce v režimu NBD onsite. |  |
| Podpora musí umožnit přístup k novým verzím FW, opravným patchům atd. |  |
| V ceně na dobu 60 měsíců. |  |
| **Požadovaná funkcionalita ve spolupráci s nabízeným zálohovacím SW** | | |
| Je požadováno, aby navržená konfigurace byla plně kompatibilní se zálohovacím softwarem pro možnost plného využití konfigurované kapacity s možností zajištění deduplikace ukládaných záloh pro celou konfigurovanou kapacitu. | |  |
| Na nabízeném serveru je možné instalovat komponenty nabízeného zálohovacího software pro zajištění zálohování virtualizace | |  |
| Na nabízeném serveru je možné instalovat jak Windows Server, tak Linux OS včetně podpory těchto OS ze strany nabízeného zálohovacího systému (včetně splnění výše uvedených podmínek). | |  |
| Konfiguraci bude možné v budoucnu doplnit o konektivitu pro připojení páskové mechaniky a zajistit tak možnost duplikace záloh na pásková média. | |  |

Gateway server

|  |  |  |
| --- | --- | --- |
| **Detailní parametry požadovaného zálohovacího serveru (1ks)** | | **Plnění požadovaných parametrů** |
|
| **Základní parametry** | 1U server určený pro montáž do standardního RACKu, duální zdroj, ližiny do racku |  |
| **Procesory (CPU)** | Požadujeme server osazený jedním procesorem. |  |
| Jeden procesor obsahující minimálně 16 fyzických jader. |  |
| Základní frekvence min. 2,0GHz. |  |
| **Paměť (RAM)** | 64 GB DDR5, možnost budoucího rozšíření na dvojnásobek. |  |
| **Diskový Řadič** | RAID řadič s podporou alespoň RAID 0/1/1+0 |  |
| **Uložiště** | * 2x 480GB SSD disk v RAID 1 konfiguraci pro instalaci OS * 2x 960 SSD disk v RAID 1 konfiguraci |  |
| **IO rozhraní (LAN/SAN)** | 4x 10/25GbE LAN |  |
| **Integrovaná vzdálená správa** | * Server musí disponovat vyhrazeným 1Gb portem pro vzdálený management. * Management musí být konfigurovatelný pro vytváření firmware sad s možností rollback při pádu aktualizace. * Server musí podporovat bez agentový vzdálený management. Vzdálený management musí podporovat standardní webové prohlížeče pro grafickou vzdálenou konzoli spolu s tlačítkem pro Virtual Power a podporovat vzdálený boot z DVD/CD/USB zařízení a být schopen uchovávat historická data o sw upgradech a patchích. * Musí být podporována vícefaktorová autentikace. * Musí být monitorovány změny v hw a systémové konfiguraci, musí být podporována rychlá diagnostika vzniklých problémů. * Musí být k dispozici dashboard s verzemi firmwaru a security doporučením (verze IPMI, notifikace k vicefaktorové autentifikaci aj.) |  |
| **Centrální Management serverů** | Centrální management pro správu všech nabízených serverů s následující funkcionalitou:   * Musí být umožněn rychlý pohled na spravované serverové zdroje. Minimální zobrazované položky Dashboardu jsou servery, firmware baselines, server hardware, inventory. * Systém musí být dostupný přes vlastní portál odkudkoliv. * Podporuje zobrazení centrálního panelu k rychlému posouzení celkového stavu zdraví spravovaných serverů, ke kterým má uživatel oprávnění * Oznámení o aktualizacích firmware s inteligentními aktualizacemi založenými pouze na rozdílech vůči stávajícímu stavu firmware na zařízení * Uživatelsky definovatelná firmware baseline pro skupiny serverů s podporou kontroly serverů souladu s touto baseline * Kontrola souladu se zvolenou firmware baseline může být spuštěna ručně, či automaticky * Skupinovou správu a aktualizaci firmware, kterou lze plánovat nebo spustit na vyžádání * Umožňuje spouštět aktualizaci firmware sériově a paralelně s možností zastavení při chybě * Možnost nastavení plně automatické aktualizace firmware OOB managementu při vydání nové verze * Možnost definovat šablony nastavení BIOS a lokální storage serveru * Automatická aktualizace katalogu dostupných firmware baseline výrobce * Automatické vytváření servisních incidentů pro události kritického charakteru * Možnost uživatelské konfigurace oznámení kritických incidentů pomocí notifikací v aplikaci a e-mailu pro každého uživatele * Možnost definice typů chyb pro zaslání emailové notifikace * Podpora pro připojení obrazu operačního systému (ISO) s možností připojení konfiguračního souboru pro bezobslužnou instalaci operačního systému * Omezení přístupu k jednotlivým serverům, nebo skupinám, na základě uživatelsky definovatelných rolí a politik * Jednotné místo pro auditní logy všech aktivit nástroje * Možnost exportu inventáře zvolených serverů do souboru * Zobrazení informací o konektivitě síťových portů v serveru při zapojení do podporovaných swichtů * Možnost definice a přiřazení značek ke spravovaným zařízením * Možnost filtrování a práce se zařízeními na základě přiřazených značek * Možnost zobrazení zprávy o dopadu na životní prostředí spravované infrastruktury – minimálně CO2, spotřeba a náklady na provoz pro jednotlivé servery. * Grafické uživatelské rozhraní a podpora pro automatizaci s pomocí REST API * Bez pevného limitu množství spravovaných serverů * Server management sw musí být od stejného výrobce, jako je výrobce serveru. |  |
| **USB porty, VGA porty** | min 3 ks USB 3.0 portů (minimálně jeden zepředu a dva zadní). |  |
| min. 1 x VGA port |  |
| **Ostatní redundantní části** | * ventilátory i zdroje – oboje musí být vyměnitelné za provozu, * napájecí zdroje s účinností minimálně 96% a výkonem min. 1000W každý |  |
| **Bezpečnost** | * Podpora UEFI Secure Boot a Secure Start * Funkce zabezpečení, která zajistí, že servery nespustí ohrožený kód firmwaru * Podpora FIPS 140-2 * Podpora Advanced Encryption Standard (AES) a Triple Data Encryption Standard (3DES) v prohlížeči * Podpora Commercial National Security Algorithms (CNSA) módu pro zabránění použité nezabezpečených algoritmů * Aktualizace bez neoprávněné manipulace – digitálně podepsané a ověřené komponenty * Secure Recovery – obnovení kritického firmwaru do známého dobrého stavu při detekci kompromitovaného firmwaru * Schopnost vrátit zpět starou verzi firmware * Podpora one-button secure erase * Integrovaný (nevolitelný) TPM (Trusted Platform Module) 2.0 * Podpora uzamykatelného čela serveru „Bezel Locking Kit“ * Podpora možnosti detekovat vniknutí do šasi serveru |  |
| **OS** | Bez operačního systému. |  |
| **Záruka a podpora** | Součástí dodávky musí být podpora výrobce v režimu NBD onsite. |  |
| Podpora musí umožnit přístup k novým verzím FW, opravným patchům atd. |  |
| V ceně na dobu 60 měsíců. |  |
| **Požadovaná funkcionalita ve spolupráci s nabízeným zálohovacím SW** | | |
| Je požadováno, aby navržená konfigurace byla plně kompatibilní se zálohovacím softwarem pro možnost vytvoření siťové Gateway zajišťující oddělení primárního prostředí a Vault infrastruktury. Tato komponenta zajistí, že nebude potřeba přímého propojení mezi těmito infrastrukturami. | |  |

### LAN switch

Z hlediska LAN infrastruktury požadujeme switch pro výše uvedenou Vault infrastrukturu sloužící primárně pro propojení jednotlivých HW komponent. Požadované parametry jsou uvedeny níže:

|  |  |  |
| --- | --- | --- |
| **Detailní parametry požadovaného LAN switche (1 ks)** | | **Plnění požadovaných parametrů** |
|
| **Provedení** | LAN switch rack-mountable o velikosti 1U |  |
| součástí dodávky musí být i ližiny do 19“ racku |  |
|  | Proudění vzduchu ve směru od zdrojů k I/O portům. |  |
|  | Minimálně 2x redundantní napájecí zdroje a redundantní ventilátory, hot swappable |  |
| **Konfigurace** | * 18x1/10/25GbE * 4x40/100GbE |  |
|  | Minimálně 8 GB RAM. |  |
|  | Interní storage - min. 16 GB. |  |
|  | Packet Buffer min. 16 MB |  |
|  | 1GbE Management port |  |
| **Propustnost a výkon** | Switching kapacita alespoň 1,7 Tbps. |  |
|  | Propustnost alespoň 1.26 Bpps. |  |
| **Napájení SAN switche** | Typ napájení: AC |  |
|  | Vstupní napětí: 230 V |  |
| **Funkcionalita** | Podpora zvýšené redundance multichassis portchannel pomocí Virtual port-channel (vPC) nebo obdobné technologie |  |
|  | Podpora standardů - 802.1D, 802.1p, 802.1Q, 802.1Qbb, 802.1Qaz, 802.1s, 802.1w, 802.3x, 802.3ad, 802.1AB |  |
|  | Podpora RDMA over Converged Ethernet (RoCEv2), Virtual routing and forwarding (VRF), OSPFv2, OSPFv3, BGPv4/v6, Equal-cost multi-path (ECMP), Policy-based routing, |  |
| **Management** | CLI  REST  Nativní management nástroje OpenSSH, SCP a FTPS  Management VRF  DHCP a v4/v6 DHCP relay |  |
| **Licence** | Dodávka musí obsahovat všechny potřebné licence pro zapojení switche v lokalitě a pro využití všech funkcí dodávaného zařízení |  |
| **Požadované SFP porty a kabely** | K LAN switchi požadujeme dodat následující moduly:   * 6x 25Gb SFP28 SR * 4x 10GBASE-T SFP+ RJ45 |  |
| **Záruka a podpora** | Součástí dodávky musí být podpora výrobce v režimu NBD onsite. |  |
| Podpora musí umožnit přístup k novým verzím FW, opravným patchům atd. |  |
| V ceně na dobu 60 měsíců. |  |

## Požadované implementační služby

V rámci dodávky požadujeme kompletní instalační a implementační službu pokrývající celé poptávané řešení. Nabízené služby musí pokrývat alespoň následující činnosti:

* Projektové vedení v proběhu celé dodávky nabízeného řešení.
* Doprava veškerého hardware do místa instalace.
* Fyzická instalace hardware do stojanových rozvaděčů Zadavatele a připojení k silovým rozvodům.
* Připojení jednotlivých komponent do LAN Zadavatele.
* Propojení veškerých dodaných komponent řešení.
* Instalace VMware clusteru a konfigurace vSAN datastore;
* Aktualizace clusteru na aktuální verzi;
* Instalace nabízeného řešení pro zálohování;
* Konfigurace zálohování včetně vybudování Vault zabezpečené lokality;
* Konfigurace zálohovacích politik pro virtuální prostředí a provozované aplikace.
* Příprava akceptačních testů pro ověření funkcionality dodávaného řešení.
* Provedení jednotlivých akceptačních testů a jejich vyhodnocení.
* Proškolení administrace řešení;
* Zpracování provozní dokumentace dodávaného řešení.

## Požadované služby v rámci standardní záruky

Součástí nabízeného řešení musí být následující služby poskytované dodavatelem v rámci standardní záruky:

* 7x24 podpora dodavatele na dodané komponenty a funkčnost dodaného řešení zahrnující následující dílčí služby:
  + „Single point of contact“ pro řešení veškerých incidentů, požadavků souvisejících s provozem celého nabízeného řešení.

Kategorie vad a SLA

|  |  |  |
| --- | --- | --- |
| Kategorie vad | Doba provozu | Reakční doba |
| Závažnost 1 – Kritická závada[[1]](#footnote-1) | 7x24 hodin | 1 hodiny od nahlášení závady |
| Závažnost 2 – Vážná závada[[2]](#footnote-2) | 7x24 hodin | 2 hodiny od nahlášení závady. |
| Závažnost 3 – Drobná vada[[3]](#footnote-3) | 7x24 hodin | 12 hodin od nahlášení závady |

* + Analýzu nahlášeného problému, jeho replikaci v laboratoři dodavatele a eskalaci na výrobce dané komponenty v případě, že dodavatel není schopen incident vyřešit ve vlastní režii.
  + Poskytování služeb prostřednictvím vzdáleného přístupu.
  + Proaktivní monitoring (24 x 7) dodaných komponent řešení se založením incidentu ze strany pracoviště technické podpory dodavatele v případě identifikace nestandardní situace nebo chybového stavu a doplněnou informací jména řešitele + kontaktu na něj v založeném incidentu.
  + Poskytování zpětné vazby ze strany dodavatele o průběhu řešení všech incidentů i prostřednictvím webového portálu.
  + Komunikace v Českém jazyce.
* Firmware/Patch Management
  + Provádění upgrade jednotlivých komponent řešení 2x ročně v pravidelných intervalech. V případě vydání kritické aktualizace bude zákazník proaktivně informován a bude dohodnuto, zda bude aktualizace aplikována mimo pravidelný cyklus.

Služby poskytované jako součást standardní záruky budou poskytovány po dobu 60 měsíců.

# Část 2 – Služby datového centra

Pro umístění nabízené infrastruktury požadujeme nabídku na níže uvedené služby datového centra.

|  |  |  |
| --- | --- | --- |
| **Požadované služby Datového centra** | | **Plnění požadovaných parametrů** |
|
| **Serverhousing a Networking** | Server housing pro technologie nabízené v části specifikující DR a zálohovací infrastrukturu. |  |
| Server housing pro technologie nabízené v části specifikující DR a zálohovací infrastrukturu. Konkrétně HW technologie nabízené pro datový trezor. |  |
| Datový okruh mezi stávajícím datovým centrem DC Faster a nabízeným datovým centrem o kapacitě 25/25Gbs včetně X-Connect v obou směrech |  |
| Internetová konektivita do nabízeného DC s kapacitou 5Gbs, 2x 10/25G port, LACP – redundantní. |  |
| **Managed services** | 10 MD práce seniorního systémového administrátora pro asistenci při instalaci a konfiguraci nabízeného řešení. |  |
| Podpora v režimu 24/7 včetně služby Remote Hands na dobu 60 měsíců |  |
| **Požadované parametry** | recovery DC musí být v jine energetické soustavě než primární DC v rámci ČR - musí splňovat parametry Tier III ve smyslu standardu **TIA-942** (Telecommunications Infrastructure Standard for Data Centers) . |  |
| recovery DC musí být propojeno dedikovaným L2 propojem s primárním DC s minimální propustností 25/25Gbs. |  |
| recovery DC musí být napájené ze dvou nezávislých větví energetické soustavy a musí být vzdáleno minimálně 180 km vzdušnou čarou od primárního DC na území České republiky |  |

1. Závada s významným dopadem na IT infrastrukturu, informační systémy a aplikace a procesy organizace. Závada způsobuje úplné nebo téměř úplné odstavení klíčových procesů nebo podporovaných systémů. Neexistuje žádné dostupné řešení ani náhrada. Příklady kritických závad: selhání informačních systémů nebo jejich částí, odstavení klíčových databází, odstavení celého systému zálohování dat, selhání obnovení kriticky potřebných dat, významné snížení výkonu celého systému, významný kybernetický bezpečnostní incident [↑](#footnote-ref-1)
2. Závada s významným dopadem na IT infrastrukturu, informační systémy a aplikace, ale bezprostředně neohrožující klíčové procesy organizace. Informační systémy a aplikace jsou částečně funkční nebo existuje dočasné řešení. Příklady závažných závad: nefunkční či jen částečné funkční funkce, zpomalení aplikace, chyba zálohování a obnovy bez bezprostředního rizika ztráty dat, ztráta vysoké dostupnosti řešení [↑](#footnote-ref-2)
3. Vada, jež nenaplňuje definici kategorie 1 a 2. Vada s minimálním dopadem na procesy organizace nebo vada bez dopadu na provoz (kosmetická vada). Celková funkčnost informačních systémů a aplikací není nijak ohrožena. Příklady drobných vad: nesprávně zobrazený prvek v rozhraní, chyba v reportu, varovná zpráva označující možný budoucí problém, drobná chyba konfigurace s minimálním dopadem na celkovou funkčnost [↑](#footnote-ref-3)