**Veřejná zakázka: Rozvoj digitalizace v Odrách III.**

**Část A - Pořízení HW infrastruktury**

**Technická specifikace včetně způsobu splnění požadavků**

*Dodavatel jednoznačně deklaruje splnění.*

Popis splnění **(zde účastník popíše způsob splnění požadavku zadavatele u všech položek, tj. žlutě vyznačené buňky).**

Výrobce (vyplňuje pouze v předdefinovaných žlutě vyznačených buňkách).

Celková cena bude vyplněna v krycím listu.

# I. Dodávka vysoce dostupného virtualizačního clusteru (HA Cluster)

Požadujeme dodávku vysoce dostupného virtualizačního clusteru (dále jen HA cluster) s automatickým restartem virtualizovaných systémů, rolí a služeb při případné poruše jednoho fyzického serveru v HA clusteru, dle před-připraveného scénáře, a to v rámci zbylých funkčních serverů. Poruchový stav HA clusteru „split-brain“ jako celku či jeho části je zcela nepřípustný, tedy minimální počet serverů v HA clusteru jsou tři. HA cluster musí být schopen plně virtualizovat systémy na platformě Microsoft Windows, BSD, Linux včetně nativní podpory kontejnerizace. Nepřipouští se možnost omezení počtu virtualizovaných systémů a kontejnerů, nebo limity přidělených zdrojů dostupných v HA clusteru. Nabízené řešení musí umožňovat hromadnou ON-Line migraci virtualizovaných systémů mezi jednotlivými servery v HA clusteru. HA cluster musí obsahovat funkcionalitu, která umožňuje pořizování neomezeného počtu zachycení aktuálních stavů virtualizovaných systémů tzv. snapshots.

Každý fyzický server (node), který bude součástí HA clusteru, musí být vybaven minimálně jedním VGA konektorem a redundantními napájecími zdroji. Celý HA cluster musí umožňovat funkcionalitu pro korektní ukončení činnosti všech virtualizovaných systémů a HA clusteru jako takového při výpadku dodávky el. energie. Systém musí umožňovat funkcionalitu komunikace mezi HA clusterem a UPS renomovaných výrobců jako např. APC, HP, Eaton, Fortron apod., která umožní korektní vypnutí všech systémů při výpadku dodávky el. energie a to dle předem definovaného scénáře. Data virtualizovaných systémů musí být uložena na SSD úložišti nebo diskovém poli (dále jen datové úložiště), s odolností proti výpadku či poruše minimálně dvou SSD disků. Celková čistá datová kapacita HA clusteru (bez systému zálohování) musí být minimálně 40 TB s tím, že paritní RAID pro ochranu dat se nepřipouští. Datové úložiště HA clusteru v režimu vysoké dostupnosti musí být vybaveno akcelerátorem / cache o minimální kapacitě 1TB. Je přípustné použít akcelerátor využívající technologii NVMe o minimální kapacitě 1TB, celý HA cluster včetně datového úložiště bude provozován v režimu vysoké dostupnosti a porucha akcelerátoru nesmí v žádném případě ohrozit integritu uložených dat. Zadavatel připouští externí diskové pole, které zcela prokazatelně zaručuje provoz celého HA clusteru v režimu vysoké dostupnosti. Za předpokladu plného osazení datového úložiště NVMe disky, nemusí být již použita žádná další cache.

Datová komunikace mezi výpočetními servery HA clusteru a datovým úložištěm musí být o minimální propustnosti 64 Gbit/s. Všechny síťové prvky pro propojení serverů v HA clusteru s datovým úložištěm musí být součástí dodávky a také plně v režimu vysoké dostupnosti. HA cluster musí umožňovat napojení ke stávající síťové infrastruktuře zadavatele z každého fyzického serveru o minimální kapacitě 2x 10Gbit DAC / SFP+ a 2x 1GbE RJ-45. HA cluster musí obsahovat funkcionalitu pro reportování poruchových stavů pomocí komunikačních kanálů SMS a email. Při výpadku internetu zadavatele musí být informace poruchového stavu zaslána alespoň jedním z uvedených komunikačních kanálů.

# II. Systém pro zálohování dat v clusteru

Systém pro automatizované zálohování dat v clusteru musí být plně kompatibilní s nabízenou virtualizační platformou, musí umožňovat de-duplikaci, kompresi a šifrování dat včetně automatické kontroly integrity provedených záloh. Systém musí umožňovat bez-výpadkové zálohování spuštěných virtualizovaných systémů v režimu zachycených stavů v HA clusteru. Systém musí obsahovat funkcionalitu pro definici plánu záloh (plánovač). Ovládání systému pro zálohování a obnovu dat musí být uživatelsky přívětivé a to pomocí grafického uživatelského rozhraní (dále jen GUI), čistě textová konzole pro ovládání zálohování a obnovu dat se nepřipouští. Využitelná kapacita primárního zálohovacího systému dat musí být minimálně 110 TB a musí být odolná proti výpadku minimálně dvou datových disků s tím, že ochrana dat paritním RAIDem se nepřipouští. Za předpokladu vybavení primárního zálohovacího systému rotačními disky, musí být jejich minimální otáčky 7200 ot/min, rozhraní SAS3 a diskový subsystém musí být vybaven akcelerátorem / cache o minimální kapacitě 1 TB. Je přípustné použít akcelerátor využívající technologii NVMe o minimální kapacitě 1TB, porucha akcelerátoru nesmí v žádném případě ohrozit integritu uložených dat. Primární systém zálohování musí být vybaven redundantními napájecími zdroji. Systém musí také umožňovat ukládání dat pomocí protokolů CIFS a NFS. Primární systém zálohování musí obsahovat funkcionalitu pro zasílání zpráv emailem o výsledku naplánovaných zálohovacích úloh.

**Disaster recovery**

Nedílnou součástí systému zálohování musí být také funkcionalita pro tzv. "Disaster Recovery" - uložení off-site zálohy, tzn. další nezávislá záloha dat, která bude umístěna v jiné lokalitě (dále DR systém). DR systém musí být plně kompatibilní s primárním systémem a musí také umožňovat de-duplikaci, kompresi a šifrování dat včetně automatické kontroly integrity provedených záloh. Obnova dat z DR systému musí být v plném rozsahu možná i bez dostupnosti dat z primární zálohy. Ovládání systému pro zálohování a obnovu musí být uživatelsky přívětivé pomocí grafického uživatelského rozhraní (dále jen GUI), čistě textová konzole pro ovládání zálohování a obnovu dat se nepřipouští. DR systém bude s primární lokalitou propojen optickou infrastrukturou zadavatele. DR systém musí být vybaven LAN konektory minimálně 2x SFP+ a 1x 1GbE a redundantními napájecími zdroji. Velikost úložiště DR systému musí být v minimální velikosti primárního zálohovacího systému a musí být odolné proti výpadku minimálně dvou datových disků. Za předpokladu vybavení zálohovacího systému rotačními disky, musí být jejich minimální otáčky 7200 ot/min, rozhraní SAS3.

DR systém musí obsahovat funkcionalitu pro zasílání zpráv emailem o výsledku plánované úlohy zálohování.

**Všechny dodané disky v rámci datové části clusteru a zálohovací části, musí být v tzv. data-center-grade kvalitě, běžně komerční SSD a rotační disky se nepřipouští. SSD disky datového úložiště musí splňovat DWPD o minimální hodnotě 2.**

# III. Dodávka Firewallu

Požadujeme dodávku vysoce dostupného Firewallu pro filtraci, řízení a analýzu provozu mezi virtualizovanými systémy v rámci HA clusteru, LAN / WAN sítí zadavatele a internetem. Záměrem zadavatele je při obnově datacentra bezpečnost perimetru svěřit výhradně na hraniční firewall, včetně zabezpečení služeb DNS. Požadujeme podporu obou typů zapouzdření GRE a GIF. Firewall musí být zkonfigurován a provozován v režimu vysoké dostupnosti. Požadujeme tedy dodávku minimálně dvou fyzických zařízení (boxů), které budou propojeny a zkonfigurovány jako vysoce dostupný Firewall (HA). Virtualizovaný Firewall jako appliance se nepřipouští. Ovládání firewallu musí být uživatelsky přívětivé pomocí grafického uživatelského rozhraní (dále jen GUI) minimálně v českém a anglickém jazyce. Pouze textová konzole pro ovládání firewallu se nepřipouští. Firewall musí být zkonfigurován tak, aby při případné poruše jednoho z boxů, druhý bezprostředně převzal všechny jeho funkce, s výpadkem služeb do 500 milisekund. Firewall musí umožňovat funkcionalitu pro sledování změn konfigurace a to pomocí GUI rozhraní (dále jen verzování). Verzování musí umožňovat funkcionalitu pro porovnávání změn v konfiguraci s možností návratu k dříve použité konfiguraci. Instalaci a implementaci firewallu musí realizovat výrobcem certifikovaný technik. Nedílnou součástí dodávky bude předání uživatelského manuálu v tištěné, nebo elektronické podobě.

# IV. Záruční a licenční podmínky

Záruka na veškerá dodaná zařízení (včetně všech síťových prvků) musí být min. 60 měsíců a to v režimu **oprava následující pracovní den v místě instalace** (tzv. 5 year NBD-FIX-On-Site).

Veškeré potřebné licence k dodanému řešení musí být trvalé. Licence formou předplatného, nájmu nebo obdobného charakteru, se nepřipouští. Z licenčního hlediska dodané řešení musí být provozuschopné i po ukončení doby udržitelnosti projektu a uplynutí záruční lhůty bez licenčních omezení či omezeních obdobného charakteru se zachováním všech požadovaných funkcionalit.

# V. Monitoring

Dodavatel musí zajistit u dodaných zařízení napojení všech systémů do monitorovacího systému dodavatele pomocí zabezpečeného datového komunikačního kanálu /např. VPN/ s evidováním a reportováním dle nastavitelných scénářů podle potřeb zadavatele. Monitorované údaje provozu musí být minimálně v tomto rozsahu sledovaných veličin:

*Stav HA clusteru a jeho nodů, obsazenost místa na discích, stav disků (SMART), teplota disků, zátěž jednotlivých CPU, využití ETH portů, zátěž diskového subsystému pro vstupně-výstupní operace (I-O), teploty jednotlivých CPU, využití RAM, propustnost portů, chybovost portů, monitoring LAN i WAN portů a celkovou zátěž firewallu, využití SWAP oddílu disků.*

Maximální perioda sběru metrik je 5 minut. Minimální doba uchování metrik je 30 dnů. Monitoring musí umožnit zasílání definovaných informací komunikačními kanály (email, SMS) dle závažnosti zjištěných veličin na definované kontakty, dle scénáře definovaného v servisní smlouvě. Dodavatel musí průběžně a pro-aktivně monitorovat stav funkčnosti dodaného řešení a navrhovat případné úpravy a opravy po dobu trvání záruční lhůty. Veškeré náklady spojené s monitoringem musí být po dobu záruční lhůty zohledněny v cenové nabídce v části "servisní smlouva".

# VI. Implementační práce

Migrace a integrace dat ze stávajícího řešení zadavatele znamená migraci dat z virtualizace KVM v současném datacentru do nového HA clusteru. Předpokládaný objem přenášených dat je do 60 TB.

Nastavení systémů zálohování dle požadavků zadavatele (zálohovací plán).

Implementace a zprovoznění firewallu bude provedena novu definicí všech pravidel (z původního řešení nedochází k přenosu stávající konfigurace). Předpokládaný objem implementačních prací firewallu je do 20h.

Poskytnutí zaškolení 2 pracovníků zadavatele v místě instalace dodávaného řešení (v prostorách zadavatele) v požadovaném rozsahu do 60hodin. Obsahem zaškolení bude seznámení pověřených pracovníků zadavatele s ovládáním všech dodaných systémů tak, aby byli následně schopni samostatné správy systémů na administrátorské úrovni.

**A) Virtualizační cluster:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Požadavek** | **minimální požadavky** | **Popis splnění** | **Název výrobce** |
| Celkový počet fyzických jader | 48 jader/cluster |  |  |
| cache | 128MB/procesor |  |
| taktovací frekvence | 3,2 GHz |  |
| VGA konektor | 1/server |  |  |
| ECC DDR4 (celá kapacita HA clusteru) | 1024 GB DDR4 ECC |  |  |
| SFP+ | 2/server |  |  |
| 1 GbE RJ-45 | 2/server |  |
| KVM over LAN (ILO) | Dedikovaný interface RJ-45/server |  |  |
| 19“ provedení, teleskopické lyžiny, redundantní napájecí zdroje | 2x PSU/server |  |  |
| Data-center grade SSD, čistá kapacita 40TB, paritní RAID se nepřipouští + 1 TB akcelerátor / cache | (SSD DWPD minimálně 2) |  |  |
| Minimální datová propustnost mezí fyzickými servery (tzv. Výpočetními nódy ) v HA clusteru a datovým úložištěm | 64 Gbit/s |  |  |
| Hromadná On-line migrace spuštěných virtuálních systémů mezi servery v HA clusteru |  |  |  |
| HA cluster musí být schopen plně virtualizovat systémy na platformě Microsoft Windows, BSD, Linux včetně nativní podpory kontejnerizace |  |  |  |
| Pořizování neomezeného počtu zachycení aktuálních stavů virtualizovaných systémů tzv.snapshots |  |  |  |
| Komunikace mezi HA clusterem a UPS |  |  |  |
| Ovládání clusteru pomocí aplikace výrobce, nebo jiný systém pro komfortní ovládání clusteru na bázi GUI. Čistě textová ASCII konzole se nepřipouští |  |  |  |
| Ovládání clusteru z nativní mobilní aplikace |  |  |  |
| Funkcionalita pro reportování poruchových stavů pomocí komunikačních kanálů SMS a e-mail |  |  |  |
| Při výpadku internetu zadavatele musí být informace poruchového stavu zaslána alespoň jedním komunikačním kanálem (SMS, email) |  |  |  |
| **Záloha dat v clusteru:** | | |  |
| Systém pro zálohování dat v clusteru plně kompatibilní s nabízenou Virtualizační platformou |  |  |  |
| Plná podpora de-duplikace |  |  |  |
| Komprese a šifrování provedených záloh virtualizovaných systémů |  |  |  |
| Ovládání zálohování pomocí aplikace výrobce, nebo jiný systém pro komfortní ovládání clusteru na bázi GUI. Čistě textová ASCII konzole se nepřipouští |  |  |  |
| Funkcionalita pro definici plánu záloh (plánovač) |  |  |  |
| Systém musí umožňovat bez-výpadkové zálohování běžících virtualizovaných systémů v režimu zachycených stavů v rámci HA clusteru |  |  |  |
| Využitelná kapacita 110 TB Datacenter SAS3 HDD 7200 RPM + 1 TB akcelerátor / cache, paritní RAID se nepřipouští | SAS3 7200 RPM - 110 TB a 1 TB akcelerátor |  |  |
| Rychlost propojení s daty v clusteru | 32 Gbit/s |  |  |
| Všechny fyzické servery musí být vybaveny funkcionalitou pro vzdálené ovládání a Monitoring Hardwaru, například ILO, KVM over LAN atd. |  |  |  |
| Komunikace mezi primárním systémem zálohování a UPS |  |  |  |
| Primární systém zálohování musí být vybaven redundantními napájecími zdroji |  |  |  |
| Systém zálohování musí obsahovat funkcionalitu zasílání zpráv emailem o výsledku naplánovaných zálohovacích úloh |  |  |  |
|  |  |  |  |
| **Disaster recovery (DR systém)** | | |  |
| Umožňuje de-duplikaci, kompresi a šifrování dat včetně automatické kontroly integrity provedených záloh |  |  |  |
| Ovládání systému pro zálohování a obnovu musí být uživatelsky přívětivé pomocí grafického uživatelského rozhraní (dále GUI), čistě textová konzole pro ovládání zálohování a obnovu dat se nepřipouští |  |  |  |
| DR systém musí být vybaven minimálně 2x SFP+ a 1x 1GbE |  |  |  |
| DR systém musí být vybaven redundantními napájecími zdroji |  |  |  |
| Velikost úložiště DR systému musí být v minimální velikosti primárního zálohovacího systému a musí být odolná proti výpadku minimálně dvou datových disků |  |  |  |
| Datacenter SAS3 HDD 7200 RPM | SAS3 7200 RPM |  |  |
| Redundantní napájecí zdroje | 2x PSU/server |  |  |
| DR systém musí obsahovat funkcionalitu zasílání zpráv e-mailem o výsledku plánované úlohy zálohování |  |  |  |

**B)** **Popis požadovaných funkcionalit poptávaného Firewallu:**

|  |  |
| --- | --- |
| **Požadavek** | **Popis splnění** |
| Transparentní cache Proxy, Reverzní Proxy pro HTTP a HTTPS včetně podpory SSL inspekce |  |
| HTTP/HTTPS antivirová kontrola |  |
| IPS (Intrusion Prevention System) / IDS (Intrusion Detection System) |  |
| Podpora integrace uživatelských a přístupových práv pomocí LDAP (Microsoft AD) a Radius |  |
| VPN site-site, server / klient (IPsec, SSL VPN) |  |
| DHCP server a DHCP relay |  |
| Integrované nástroje pro analýzu a monitoring datového provozu |  |
| 802.1Q VLAN |  |
| Konfigurace přes webové rozhraní v Českém a Anglickém jazyce + lokální a vzdálená SSH konzole - Podpora protokolů IPv4 a IPv6 |  |
| Pokročilé filtrování provozu dle mnoha pravidel (TCP/ UDP, GRE, VLAN-y+, GEOIP, Operační systémy, VPN skupiny, URL atd..) |  |
| Podpora IP a URL aliasů pro vytváření pravidel |  |
| NAT (Přesměrování portů, 1:1 NAT, Odchozí NAT, atd.) |  |
| Několikanásobná podpora pro WAN rozhraní (několik internetových přípojek) |  |
| Několikanásobná podpora pro LAN rozhraní (DMZ atd.) |  |
| Load Balancing – rozložení zátěže mezi několik internetových přípojek |  |
| Server inbound load balancing – rozložení zátěže mezi servery v DMZ. (mail servery, Terminály atd.) |  |
| Vysoká dostupnost (HA) – minimálně 2 HW boxy |  |
| Podpora NEXTGen funkcionalit |  |
| WEB security |  |
| Policy based filtering |  |
| User based filtering |  |
| Policy based QoS |  |
| PPPoE server / klient |  |
| QOS a traffic shaper |  |
| Přehledné grafy a historie datového provozu Firewallu v GUI |  |
| Podpora pro Captive Portal |  |
| DNS server a DNS relay |  |
| Podpora Dynamic DNS, DNSSec, DNS over SSL |  |
| Virtuální rozhraní pro VLAN, LAGG/LACP, GIF, GRE, PPPoE/PPTP/L2TP/PPP a síťové mosty |  |
| Podpora pro transparentní PROXY server |  |
| Podpora pro antivirovou kontrolu HTTP/HTTPS provozu |  |
| Verzování konfigurace |  |
| Aplikace pro kompletní analýzu datového provozu firewallem - Otevřený protokol pro monitoring sítí na základě IP toků, portů, statistik, atd. |  |
| Výrobcem certifikovaný technik |  |
| **Minimální požadavky na konfiguraci Firewallu :** | |
| Minimálně 10 x 1 GbE LAN porty + 4x SFP+ |  |
| Propustnost Firewallu minimálně 1000 Mbit/s s maximální latencí do 5ms při 500 statických pravidlech a aktivní IDS. |  |
| Redundantní napájecí zdroj (2x PSU/box) |  |
| Veškeré potřebné licence k dodanému řešení musí být trvalé. Licence formou předplatného, nájmu nebo obdobného charakteru, se nepřipouští. Z licenčního hlediska dodané řešení musí být provozuschopné i po ukončení doby udržitelnosti projektu a uplynutí záruční lhůty bez licenčních omezení či omezeních obdobného charakteru se zachováním všech požadovaných funkcionalit |  |

**C)** **Popis požadovaných prací:**

|  |  |  |
| --- | --- | --- |
| **Práce - požadavek** | **ks** | **Popis splnění** |
| Konfigurace zálohování | do 3 hod |  |
| Implementace firewallu | do 20hod |  |
| Migrace a integrace dat ze stávajícího virtualizačního clusteru | 60 TB |  |
| Školení pro správce (2 osoby) v místě instalace/školící místnosti dodavatele | 60 hodin |  |