

SPECIFIKACE PŘEDMĚTU ZAKÁZKY

Název veřejné zakázky	Školní server
Číslo akce	110-24/2018/RK
Název příspěvkové organizace (zadavatel veřejné zakázky)	Střední průmyslová škola strojírenská a Jazyková škola s právem státní jazykové zkoušky, Kolín IV, Heverova 191
Sídlo příspěvkové organizace	Heverova 191, 28002 Kolín IV
IČ příspěvkové organizace	48665860
Jméno a příjmení ředitele PO	Ing. Jaromír Kratochvíl
Kontaktní osoba zadavatele	Ing. Jaromír Kratochvíl 321 743 023/321 743 022 kratochvil@sps-ko.cz

1) Předmět zakázky

Předmětem zakázky je dodávka 1ks serveru, 1ks hardware pro zálohování, software pro virtualizaci, software pro zálohování, software pro e-mailový server, 1ks firewall včetně instalace a konfigurace (náhrada za současný Firewall MikroTik), převod současných aplikací a dat na nový server, přemístění doménového kontroleru na nový server, převod e-mailových služeb a dat na nový server, implementaci a zaškolení na nabízené a dodávané produkty.

2) Specifikace předmětu zakázky

A) Server (minimální požadavky na server):

- Volně stojící (tower), dvousocketový server
- Jedenkrát procesor s minimálními parametry: 12 jader, taktovací frekvence 2.1 GHz, 18 MB L2 cache, 85W.
- Minimálně 24 paměťových slotů, podpora pamětí DDR4, 2600 MT/s, umožňuje rozšiřitelnost RAM na minimálně 1,5 TB.
- Kapacita instalované RAMM 64GB, DDR4-2666.
- 12Gb SAS RAID řadič s podporou RAIDu 0/1/5/6/10/50/60 s cache minimálně 2GB, která je zálohována baterií nebo flash pamětí. Musí umožňovat přístup na disky v RAID i HBA módu souběžně. Podpora pro rozšiřování kapacity, rozšiřování logický disků a migrace RAID úrovně. Podpora pro integrované šifrování dat. Podpora pro CACHING dat na lokální SSD. Řadič nezabírá PCIe slot.
- Minimálně 8 pozic pro 2,5" hot-swap SAS/SATA/SSD disků. Možnost rozšíření až na 24 pozic pro 2,5" hot-swap pevné disky.
- Disky musí mít rámečky vybaveny indikátorem proti vytažení disku, na kterém se provádí datové operace nebo musí být takový disk proti případnému vytažení blokován.
- Osazeno 4x minimálně 600 GB SAS disk 2,5" 15k otáček, digitálně podepsaný firmware.
- Osazeno 2x minimálně 300 GB SAS disk 2,5" 15k otáček, digitálně podepsaný firmware.
- Minimálně 6x USB porty 3.0, z toho minimálně 1x interní pro aplikační klíče.
- Slot pro interní flash kartu (SD, microSD) pro boot hypervizoru.
- 4x 1Gbit LAN porty integrované na základní desce.

- Interní DVD-RW optická mechanika.
- 2x Hot plugové napájecí zdroje s redundancí napájení 1+1, minimální požadovaný výkon jednoho zdroje je 800W.
- Redundantní ventilátory.
- Dedikovaný management port.
- Klávesnice s českými znaky, optická myš.
- Předplacená tříletá servisní podpora s opravou v místě instalace serveru a se zahájením opravy následující pracovní den.
- Licence pro správu serveru a management SW umožňující:
 - Řízení přístupových práv k centrální části SW a k management nástrojům pomocí účtů Active Directory domény, autentizace uživatele PINem a certifikátem.
 - Virtuální KVM (tj. převzetí textové i grafické konsole serveru a zajištění přenosu povelů z klávesnice a myši vzdáleného počítače).
 - Zapnutí, vypnutí a restart serveru na dálku.
 - Namapování vzdálených medií Floppy/CD, image souborů a adresářů.
 - U grafické konsole rozlišení minimálně až 1600x1200.
 - Možnost využití běžných www prohlížečů integrovaných v desktopovém OS pro správu serverů (IE, Firefox).
 - Kódování Advanced Encryption Standard (AES) a Triple Data Encryption Standard (3DES) pro zabezpečení komunikace s běžnými www prohlížeči.
 - CLP a XML rozhraní pro skriptování.
 - Možnost vyvolat NMI přerušení nedostupného OS.
 - Možnost zasílání proaktivních hlášení o možných chybách v systému pomocí SNMP a také na uživatelsky definovanou emailovou adresu.

B) NAS zálohovací systém (specifikace zálohovacího systému NAS):

- Počet šachet pevného disku: 2.
- Provedení skříně: Desktop.
- Připojitelnost zálohovacího systému: RJ-45 / 1 Gbit/s, šifrování dat na záloze.
- V ceně dodávky bude 2x disk, každý o kapacitě min. 1TB určený pro režim provozu 24/7 v NAS úložných systémech.
- Požadované minimální parametry zálohovacího systému:
 - Hardwarové šifrování AES-NI.
 - Rychlost šifrovaného čtení 113 MB/s, rychlost šifrovaného zápisu 112 MB/s.
 - HotSwap disky vyměnitelné za provozu.
 - Rozhraní: USB 3.0, USB 2.0, RJ45 – gigabit ethernet.
 - Včetně systému manageru NAS.
 - Frekvence CPU minimálně 2,4 GHz, 2 jádra.
 - Paměť: min. 2GB rozšiřitelná na min. 6GB.
 - Interní HDD/SSD: Kompatibilní typ disku: 3.5" SATA HDD, 2.5" SATA HDD, 2.5" SATA SSD.
 - Maximálně interní kapacita: 24 TB (2 X 12 TB HDD) (Kapacita se může lišit podle typu pole RAID).
 - Záruka tři roky.

C) Software pro virtualizaci

- Licence na software pro virtualizaci včetně licence pro konzoli centralizované správy, s licenčním pokrytím na minimálně 1 procesor a předplacenou podporou (technické incidenty, aktualizace) na 3 roky v ceně dodávky.

- Software pro virtualizaci musí splňovat minimálně tyto požadavky:
 - Platforma pro vysoce výkonnou virtualizační vrstvu, která umožňuje více virtuálním strojům sdílet zdroje výpočetní (computing), síťové (networking) a datové na jediném fyzickém serveru.
 - Licence bez omezení RAM a CPU na virtualizovaný server.
 - Centrální management fyzických virtualizačních serverů (host) a virtuálních serverů (guest)
 - Memory ballooning.
 - Možnost alokace systémových prostředků jednotlivým virtuálním strojům nebo jejich skupinám.
 - Podpora PV, BT, HW (paravirtualization, binary translation, hardware assist) vizualizace
 - Umístění kompletního prostředí včetně OS a aplikací do virtuálních strojů bez závislosti na provozovaném hardware.
 - Symetrický multiprocessing zlepšující výkonnost virtuálního stroje a umožňující, aby jediný virtuální stroj využíval několik virtuálních procesorů současně.
 - Konzole centralizované správy umožňuje rychlé zprovoznění služeb, centralizované řízení a sledování výkonnosti. Obsahuje vestavěné monitorovací nástroje, funkcionalitu P2V migrace (konverze fyzického stroje na virtuální), na průvodcích založené vytváření a nasazení systémů a mnoho další funkcionality.
 - Update Manager poskytuje automatizovanou správu záplat pro virtualizované servery.
 - funkce Virtual Symmetric Multiprocessing umožňuje používat virtuální stroje, které mají minimálně 8 virtuálních CPU (vCPU).
 - Nástroj pro rychlou konverzi fyzických serverů a virtuálních strojů třetí strany ve virtuální stroje v nabízeném produktu.
 - Bezpečné API umožňující použití bezpečnostních produktů, které pracují ve spojení s virtualizační vrstvou, aby tak poskytly vyšší úroveň zabezpečení virtuálních strojů, než je možné s fyzickými servery.
 - Hardware kompatibilita je možná s nejširším spektrem 32- a 64-bitových serverů a OS, úložišť a síťových zařízení a firemních nástrojů pro správu.
 - Předplacená podpora (technické incidenty, aktualizace) na dobu pět let v ceně dodávky.

D) Software pro zálohování

- Licence s licenčním pokrytím na 1 procesor a předplacenou podporou (technické incidenty, aktualizace) na dobu 5 let v ceně dodávky.
- Minimální požadavky:
 - Vyhledání a obnova všech typů objektů Active Direstory bez nutnosti instalace agenta. Obnova jednotlivých uživatelských a počítačových účtů prostřednictvím exportu ve formátu LDIFDE nebo obnovy zpět do AD i možnost obnovy hesel.
 - Obnova celých virtuálních strojů, ale i jednotlivých souborů a aplikačních položek jedním kliknutím přes webové uživatelské rozhraní.
 - V ceně management pro správu záloh.
 - Zálohování pouze části VM (file-selective backup).
 - Reportování záloh (včetně hodnocení konfigurace záloh).
 - Obnova celého virtuálního počítače na původním nebo jiném hostiteli, včetně funkce rychlého vrácení akce zpět pro obnovení pouze změněných bloků.

- Obnova nebo migrace onsite virtuálních počítačů se systémem Windows nebo Linux, fyzických serverů a koncových bodů přímo do prostředí Microsoft Azure.
- Rychlé přírůstkové zálohování jednotlivých virtuálních počítačů s existující úlohou zálohování.
- Vytváření záloh virtuálních počítačů na úrovni bitových kopií konzistentních v aplikacích se zpracováním s ohledem na aplikace (včetně zkracování protokolů transakcí).
- Integrovaná deduplikace, komprese a eliminace swap souborů.
- Zabezpečení dat záloh a síťových přenosů pomocí komplexního 256 bitového šifrování AES bez nepříznivého vlivu na integrované funkce komprimace či snížení kompresního poměru.

E) Operační systém serveru

- Škola aktuálně používá na serverech operační systém Windows 2008 Server včetně nainstalované role Active Directory Domain Services. U operačního systému dodávaného k novému serveru požadujeme plnou kompatibilitu s již instalovaným prostředím na škole a dodávku licencí v tomto rozsahu:
 - Licence operačního systému pro nabízený server (pro 4VM) + 200 uživatelských licencí pro stanice.

F) Mail server

- Škola aktuálně používá nepodporované 10let zastaralé e-mailové služby na nepodporovaném zastaralém OS a serveru Linux.
- Požadujeme dodání nového e-mailového serveru (software) s 30 mail účty. Uživatelé budou na stanicích jako klienta používat MS Outlook 2010 a vyšší.
- Požadavky na e-mailový server:
 - Propojení s klientem Microsoft Outlook pomocí protokolu MAPI over http.
 - Funkce pro plánování schůzek a přidělování úkolů.
 - Zahrnuje transportní služby, které garantují směřování a doručení poštovních zpráv.
 - Zahrnuje služby klientského přístupu, které umožňují připojení klientů různými protokoly.
 - Zahrnuje služby pro Unified Messaging (UM) pro práci s hlasovými zprávami a propojení s telefonním subsystémem.
 - Obsluhuje databáze poštovních schránek.
 - Provázání serverových technologií nabízeného e-mail serveru s SharePoint Server 2016 a Office Online Server.
 - Automatické nastavení práv pro úpravu MS Office dokumentu všem příjemcům (je možné práva změnit) a do e-mailu je vložen pouze odkaz na dokument formou ikony.
 - Synchronizace dat z poštovní schránky do mobilních zařízení. Synchronizace složky Koncepty.
 - Možnost synchronizovat kalendářové události včetně vložených příloh.
 - Funkce pro umožnění smazat pouze data z Mail Serveru místo kompletního výmazu zařízení.
 - Při potvrzování schůzky možnost i na mobilním zařízení (s Windows Mobile, Apple iOS, Android) navrhnout nový termín konání schůzky.
 - Podpora DLP (Data Loss Prevention) včetně možnosti DLP, a to jak v rámci zadaných typů citlivých informací, které umí Mail Server rozpoznat, tak i v množině akcí, které se spustí po zjištění možného úniku citlivých informací. Mezi

podporované typy detekovatelných informací patří i podpora údajů z českého občanského průkazu, konkrétně rodného čísla.

- Funkce, pomocí které lze zařídit, že zprávy jsou na Mail Serveru nesmazatelné a jsou kdykoliv dohledatelné auditorem.

G) Firewall

- Požadujeme dodání nového firewallu splňujícího následujícími minimálními parametry:
 - Počet 1GE metalických síťových rozhraní (RJ45 10/100/1000) pro firewallové funkce - minimálně 4x.
 - Počet 1GE optických síťových rozhraní (SFP) pro firewallové funkce – minimálně 2x.
 - Počet management rozhraní (RJ45) – minimálně 1.
 - Podpora LACP (802.3ad) na minimálně 4 portech stejného typu.
 - Velikost max. 1U.
 - Možnost rozšíření o druhý napájecí zdroj (interní nebo externí).
 - Lokální úložiště (nerotační technologie) min 128GB.
 - Podpora IPv6 pro všechny funkce.
 - Podpora NAT64/NAT46.
 - Výkonnost FW shodná pro IPv4 i IPv6.
- Minimální závislost výkonu firewallu na velikosti paketů:
 - Propustnost FW (stavové filtrování, UDP paket) minimálně 4 Gbps (měřeno na paketech o velikosti 1518 B).
 - Výkonnost FW na malých paketech (64 B) nesmí klesnout pod 57% výkonnosti naměřené na velkých paketech.
- Propustnost FW paketů za sekundu - minimálně 6 Mpps.
- Latence firewallu (64 B UDP paket) - maximálně 3 μ s.
- Počet naráz otevřených spojení - minimálně 1,3 M.
- Počet nových spojení za sekundu - minimálně 30 000
- Propustnost IPSEC VPN - minimálně 2,5 Gbps.
- Propustnost SSL VPN min 200 Mbps.
- Propustnost NGFW (IPS + Application control; traffic mix) - minimálně 360 Mbps.
- Propustnost IPS (měřeno na http komunikaci) – minimálně 1,5 Gbps
- Podpora virtualizace (na dané HW appliance) minimálně 10.
- Součástí dodávky musí být licence na minimálně 10 virtuálních kontextů, včetně kompletní UTM funkcionality ve všech kontextech.
- Režim vysoké dostupnosti (L2 HA, tj. virtuální MAC adresy).
- Podpora Active Active i Active Passive HA, full mesh HA, synchronizace stavové tabulky mezi nody clusteru.
- Podpora VRRP.
- Podpora L2 (transparentní) režimu i L3 (NAT/Router) režimu.
- Podpora multicast, včetně routování a firewall funkcí (tvorba multicast FW politiky).
- Podpora VPN: SSL (portálový režim, tunelový režim), IPSEC (IKE, manual key, certifikát, gateway to gateway, hub and spoke, dial up konfigurace, internet browsing konfigurace, podpora více tunelů – redundantní VPN, možnost VPN v L2 – transparentním režimu ukončená na management rozhraní, podpora IPv6, podpora dynamických routovacích protokolů - OSPF), PPTP, L2TP, GRE.
- Možnost nastavovat firewall politiku na základě geografických údajů – GeoIP

- Detekce klientského zařízení, možnost nastavovat firewall politiku na základě typu klientského zařízení (telefon, tablet, PC) včetně operačního systému (Android, iPhone, ...) bez nutnosti instalovat klienty na koncové stanice.
- Podpora firewall pravidel na základě identity uživatele pro MS AD prostředí – nastavení bezpečnosti uživateli na základě členství v AD skupině na doménovém kontroléru.
- Funkce Load Balancing - možnost rozdělování zátěže směřující na virtuální IP na reálné servery, podpora health check funkcí, podpora SSL offload.
- Podpora centrální NATovací tabulky, stavová inspekce SCTP komunikace.
- UTM funkce, možnost výběru mezi proxy režimem (buffer) nebo flow režimem (inspekce on-the-fly), zejména pro antivirovou/antimalware kontrolu.
- Antivirová/antimalware kontrola pro vybrané protokoly, možnost volby různých databází (např. minimální, standardní a extrémní) kvůli optimalizaci výkonnosti, podpora archivace škodlivého obsahu, podpora protokolu ICAP pro offload AV engine, možnost detekce tzv. Grayware (rootkit, malware, spyware, keylogger, atd).
- Automatická aktualizace signatur ze strany výrobce po dobu udržitelnosti projektu.
- Email filter - jednoduchá antispamová a antivirová inspekce elektronické pošty.
- Aktualizace signatur ze strany výrobce po dobu udržitelnosti projektu.
- Web Filter - založená na kategorizaci webového obsahu, možnost monitorování navštívených kategorií na uživatele či skupinu, možnost kvóty - uživatel může navštěvovat určitou kategorii jen po určitou dobu během dne. Automatická aktualizace signatur ze strany výrobce po dobu udržitelnosti projektu.
- Cloud Sandboxing v ceně dodávky.
- Podpora ochrany pro mobilní zařízení - funkce zajistí prohledávání datového toku i na známé signatury pro útoky na připojená mobilní zařízení (BYOD - Bring Your Own Device).
- Data Leak Prevention s funkcí document fingerprinting (běžící pouze na firewallu, tedy bez nutnosti instalovat klientský software na koncové stanice).
- SSL dekrypce/offload - možnost kontroly komunikace v SSL šifrovaných protokolech (HTTPS, IMAPS, POP3S,...).
- DoS Policy prevence proti základním útokům typu DoS, včetně syn proxy.
- Ověřování uživatelů proti LDAP, Active Directory, Single Sign On, Radius, TACACS+, Ověřování na základě certifikátu, Dynamické profily - možnost přiřadit konkrétní profil uživateli na základě jeho ověření.
- Dynamické routování:
 - RIP, BGP, OSPF.
 - Policy rating.
- Traffic Shaping (QoS, prioritizace atd.).
- Podpora VoIP, SIP včetně zabezpečení, rate limiting, analýzy protokolu.
- WAN optimalizace (optimalizace vybraných protokolů, byte caching), Web Cache, Reverzní proxy, WCCP.
- Funkce Explicitní Proxy, včetně autentizace v síti MS AD protokolem Kerberos.
- Podpora funkce wireless kontroleru, tedy možnost centrálně spravovat tenké wifi AP v počtu minimálně 32 AP (16 AP v tunnel-módu).
- Bezdrátová síť, resp. její SSID musí být plně integrováno do managementu firewallu a umožňovat nasazení všech bezpečnostních funkcí popsanych v tomto dokumentu (firewall, antivirová/antimalware kontrola, IPS, Application Control, ...).

- Bezdrátová síť musí podporovat roaming klientů za použití pre-cachingu uživatelských klíčů a detekci a potlačení neautorizovaných AP (rogue AP detection, off-wire i on-wire).
- Podpora silné autentizace uživatelů - podpora pro generátor jednorázových hesel (OTP) - Token pro dvou-faktorovou autentizaci, podpora certifikátů pro ověření uživatelů (možno jako interní součást FW nebo jako externí systém - například RADIUS server).
- Předplacená technická podpora výrobce a aktualizace v režimu 24/7 po dobu jednoho roku.

H) Instalační služby

- Součástí dodávky a cenové nabídky bude kompletní instalace a zprovoznění dodávaných produktů, nastavení virtualizace, serveru, instalace nabízených položek. Dále bude součástí dodávky zaškolení na administraci dodaných produktů v rozsahu 8 hodin.
- Součástí dodávky je i kompletní přenesení fyzického doménového kontroleru (nyní Windows server 2008 R2) do virtuálního prostředí. Dále kompletní konfiguraci virtuálního prostředí a konfiguraci zálohování tohoto prostředí, tak aby byly zaručeny aplikačně konzistentní zálohy virtualizovaných serverových operačních systémů, převod uživatelských dat a účtů (popř. jejich nové založení) na nový server, převedení e-mailových schránek a jejich dat na nové dodávané e-mailové prostředí.
- Celá dodávka musí obsahovat všechny HW komponenty a veškeré potřebné licence a servisní podporu výrobce na dobu dle výše uvedených požadavků. Žádné z nabízených řešení nesmí být v době podání nabídky v režimu end of sales/end of support. Všechny požadované funkce musí být v době podání nabídky součástí stabilní verze operačního systému/firmware, funkce zařazené na tzv. roadmapu nebudou akceptovány.
- Nabízený server musí být od výrobce s jednotnou servisní podporou v jednom místě v češtině a v České republice.
- Nabídnuto může být pouze zařízení nové, nikde před tím nepoužívané.
- Nesplnění jakéhokoliv z požadovaných a zde uvedených parametrů bude důvodem k vyloučení uchazeče z procesu hodnocení nabídek, respektive k nepřevzetí dodávky Zadavatelem.
- Dodavatel je povinen nacenit a dodat i případné práce, které nejsou přímo v této zadávací dokumentaci zmíněny, ale jsou pro řádné a funkční zprovoznění předmětu této zakázky nezbytné a o nichž dodavatel mohl nebo měl vzhledem ke své odbornosti vědět.

V Kolíně dne 5. prosince 2018.

**Střední průmyslová škola
strojírenská a Jazyková škola
s právem státní jazykové zkoušky,
Kolín IV, Heverova 191**


Ing. Jaromír Kratochvíl