Příloha č. 1 Zadávací dokumentace - Technická dokumentace zadavatele

Příloha č. 1 Kupní smlouvy - Technická dokumentace kupujícího

# Technická specifikace zadavatele (kupujícího)

Zadavatel požaduje dodávku jednotlivých komponent dle této technické dokumentace včetně příslušenství v níže uvedené minimální specifikaci.

Musí se jednat o zařízení nová, nepoužitá, nerepasovaná a určená pro prodej v České republice.

Součástí dodávky níže uvedených technologií budou i dále uvedené služby.

Součástí dodávky bude dále dodávka dokumentace a nezbytné zaškolení administrátorů v prostředí kupujícího k běžnému provozu a ovládání dodaných technologií včetně specifik a konfigurace provedené v prostředí kupujícího.

Nabízené zboží musí být standardní, běžně dostupné a určené k produkčnímu použití.

Není dovoleno použití beta-verzí, kódu s custom úpravami či neoficiálních verzí.

Veškeré nabízené zboží musí být pokryto oficiálním supportem, přičemž požadavek na provedení bezplatného servisního zásahu musí být možné kdykoliv vznést přímo na výrobce zařízení.

Veškeré deklarované funkce a technické parametry nabízeného zboží musí být dostupné nejpozději dnem podání nabídky.

Deklarované funkce a technické parametry nabízeného zboží musí být ověřitelné prostřednictvím oficiálních datasheetů, release notes či manuálů vydaných výrobcem.

Užité pojmy níže:

* NBD – další pracovní den, tzn. například realizace opravy zařízení nejpozději další pracovní den od nahlášení
* x BD – x pracovních dnů, tzn. například realizace opravy zařízení nejpozději poslední pracovní den dané lhůty od nahlášení
* on-site – realizace například opravy zařízení v místě dodávky

Z důvodu kompatibility se stávající infrastrukturou a proškolených správců počítačové sítě, mohou být v zadávací dokumentaci uvedeny konkrétní značky výrobků, nebo určitý výrobce. Tyto důvody jsou vždy uvedeny v konkrétní části specifikace tam, kde dochází k uvedení konkrétního produktového názvu. V souladu s § 89 odst. 6 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, zadavatel připouští možnost dodávky rovnocenného řešení, které však musí zajistit celý komplex služeb, který je kompatibilitou vyžadován, tedy komplexní řešení agendových informačních systémů nad touto platformou vybudovaných a provozovaných, které předmětnou infrastrukturu užívají a slouží k výkonu veřejné správy zadavatele.

**Propojení zařízení – SFP moduly a kabely**

Všechny dodané technologie musejí být v rámci dodávky propojeny odpovídajícím způsobem a technologií, tedy zejména pro všechny síťové karty jednotlivých zařízení musejí být dodány i SFP a obdobné moduly a kabely do serverovny kupujícího, které takové propojení v kvalitě požadované u každého ze zařízení umožní. V případě 10Gbit karet musí být dodány SFP prvky a kabely umožňující využití této maximální rychlosti karty, v případě jiných rychlostí toto pravidlo musí být dodrženo stejně.

**Plnění jednotlivých komponent dle specifikace níže je požadováno v následujícím rozsahu a to včetně příslušenství**

|  |  |
| --- | --- |
| **Položka plnění** | **Počet kusů** |
| Firewall s příslušenstvím | 2 |
| Přístupový přepínač s příslušenstvím typ A | 10 |
| Přístupový přepínač s příslušenstvím typ B | 8 |
| Přístupový přepínač s příslušenstvím typ C | 4 |
| Licence SW centrálního managementu + 802.1X | 1 |
| Přístupové wifi body s příslušenstvím | 15 |
| Záložní zdroj pro aktivní prvky s příslušenstvím | 13 |
| Nástroj pro logování infrastruktury | 1 |
| Produkční servery s příslušenstvím | 2 |
| Management server s příslušenstvím | 1 |
| Licence OS serverů | 2 |
| Licence řízení hypervisoru pro management server | 1 |
| Licence hypervizoru pro virtuální servery | 3 |
| Klientské licence operačních systémů | 115 |
| Licence SW pro diskovou virtualizaci | 2 |
| Záložní zdroj pro servery s příslušenstvím | 2 |
| Páteřní přepínač s příslušenstvím | 2 |
| Backup server s příslušenstvím | 1 |
| Licence OS BackUp a management serveru | 2 |
| Bezpečné datové úložiště | 1 |
| Pásková knihovna | 1 |

**Obsah**

[1 Technická specifikace zadavatele (kupujícího) 1](#_Toc146030445)

[2 Firewall s příslušenstvím 4](#_Toc146030446)

[3 Přístupový přepínač s příslušenstvím typ A 6](#_Toc146030447)

[4 Přístupový přepínač s příslušenstvím typ B 8](#_Toc146030448)

[5 Přístupový přepínač s příslušenstvím typ C 10](#_Toc146030449)

[5.1 Příslušenství přístupových přepínačů 12](#_Toc146030450)

[6 Licence SW centrálního managementu + 802.1X 12](#_Toc146030451)

[7 Přístupové wifi body s příslušenstvím 13](#_Toc146030452)

[8 Záložní zdroj pro aktivní prvky s příslušenstvím 14](#_Toc146030453)

[9 Nástroj pro logování infrastruktury 15](#_Toc146030454)

[10 Produkční servery s příslušenstvím 21](#_Toc146030455)

[11 Management server s příslušenstvím 22](#_Toc146030456)

[12 Licence OS produkčních serverů a licence OS BackUp a management serveru 24](#_Toc146030457)

[13 Licence řízení hypervisoru pro management server 24](#_Toc146030458)

[14 Licence hypervizoru pro produkční servery 24](#_Toc146030459)

[15 Licence SW pro diskovou virtualizaci 25](#_Toc146030460)

[16 Záložní zdroj pro servery s příslušenstvím 25](#_Toc146030461)

[17 Páteřní přepínač s příslušenstvím 26](#_Toc146030462)

[18 Backup server s příslušenstvím 28](#_Toc146030463)

[19 Bezpečné datové úložiště 29](#_Toc146030464)

[20 Pásková knihovna 31](#_Toc146030465)

[21 Požadavky na instalační a implementační práce 31](#_Toc146030466)

[21.1 Specifikace konkrétních instalačních a implementačních požadavků 32](#_Toc146030467)

[21.2 Obecné požadavky 33](#_Toc146030468)

[21.3 Požadavky na předimplementační analýzu 34](#_Toc146030469)

[21.4 Požadavky na zpracování prováděcí dokumentace 34](#_Toc146030470)

[21.5 Požadavky na zajištění projektového řízení 34](#_Toc146030471)

[21.6 Požadavky na zaškolení 35](#_Toc146030472)

[21.7 Požadavky na provedení zkušebního provozu a akceptačních testů 35](#_Toc146030473)

[21.8 Další požadavky na záruky, záruční servis a další podmínky v rámci záruky 35](#_Toc146030474)

[22 Harmonogram plnění 35](#_Toc146030475)

[23 Návaznost na projektový záměr kupujícího 36](#_Toc146030476)

# Firewall s příslušenstvím

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky.

| Parametr | Popis minimální úrovně parametru |
| --- | --- |
| Základní požadavky | HW appliance (VM appliance ani software řešení není akceptovatelné) |
| Podpora režimu vysoké dostupnosti minimálně jako active/active a active/passive, cluster o dvou fyzických zařízeních |
| Velikost max. 1RU |
| Podpora duálního napájení (redundantní zdroj) |
| Minimálně 2x10 GbE SFP+ sítová rozhraní |
| Minimálně 4x Shared Port Pairs, 8x GE SFP síťová rozhraní |
| Minimálně 18x 1 GbE RJ45 síťová rozhraní |
| Management rozhraní 1x 1 GbE RJ45 a sériový konzolový port |
| Výkonové požadavky | Minimální propustnost firewallu pro IPv4 i IPv6 provoz 16Gbps (měřeno na UDP komunikaci o paketech s velikostí 512 B) |
| Počet současně navázaných spojení firewallu min. 1 500 000, počet nových spojení za sekundu min. 50 000 |
| Celková propustnost IPSEC VPN min. 10Gbps |
| Propustnost SSL VPN min. 1Gbps |
| Propustnost funkce SSL inspekce min. 1Gbps |
| Počet CPS u spojení kontrolovaných pomocí SSL inspekce min. 1500 (spojení za sekundu) |
| Propustnost funkce IPS min. 2,5 Gbps (reálná hodnota, měřeno na běžném provozu – real world traffic, včetně logování) |
| Propustnost funkcí next generation firewallingu (stavový firewall, IPS, analýza aplikací) min. 1,5Gbps (reálná hodnota, měřeno na běžném provozu – real world traffic) |
| Propustnost funkcí ochrany před hrozbami (stavový firewall, IPS, analýza aplikací, ochrana před škodlivým kódem) min. 1Gbps (reálná hodnota, měřeno na běžném provozu – real world traffic) |
| Udávaná latence firewallu (udp provoz) max. 5 μs |
| Min. počet současně připojených uživatelů SSL VPN 500 |
| Min. počet site-to-site IPSEC tunelů 16000 |
| Funkční požadavky | Grafické konfigurační rozhraní (např. webový prohlížeč) a příkazový řádek bez omezení na počet administrátorů |
| Bezpečnostní funkce obecně označované jako Next Generation Firewall |
| Podpora virtualizace na daném HW, vytváření a provozování tzv. virtuálních kontextů – min. 10 virtuálních kontextů v ceně zařízení; každý virtuální kontext musí pracovat izolovaně, možnost propojovat jednotlivé virtuální kontexty pomocí interních virtuálních propojů bez nutnosti použití fyzických interface |
| Podpora stavového firewallingu pro IPv4 i IPv6, podpora NAT 64/46 |
| Možnost nasazení ve všech z následujících režimu (kombinace možné pomocí použití různých režimů pro různé virtuální kontexty): L2 bridge režim (inline), L3 router/NAT režim (inline), explicitní proxy (inline/out of path), transparentní proxy (inline) |
| Plnohodnotná správa z lokálního management rozhraní (a to i v případě využití nástroje centrální správy, neboť i v takovém případě musí být možné firewall, resp. firewall cluster, plnohodnotně konfigurovat ve chvíli, kdy z jakéhokoliv důvodu centrální správa nebude dostupná) |
| Ověřování identity uživatelů (možnost napojení na MS Active Directory, LDAP, RADIUS, Kerberos), práce s identitou uživatele v bezpečnostní politice firewallu v režimu tzv. Single Sign On |
| Podpora lokální databáze a vzdálené databáze (RADIUS, LDAP, TACACS+, SAML, Kerberos) pro ověřování uživatelů |
| Ověřování uživatelů pomocí SSO funkcionality pomocí RADIUS Single Sign On a AD pollingu |
| Funkce QoS, traffic shaping a SD-WAN minimálně v režimu vytvoření overlay a underlay virtuálních sítových rozhraní zahrnující fyzické propoje, IPSEC tunely či jiná rozhraní s možností definice pravidel pro řízení směrování, strategie využívání jednotlivých linek současně a monitorování stavu jednotlivých linek |
| Podpora funkcí VPN brány ‐ IPSec VPN (dle platných standardů pro možnost propojení se zařízeními třetích stran); - SSL VPN pro klientský přistup s tunelovacím režimem včetně klienta pro osobní počítač i mobilní platformy, portálový režim pro bezklientský přistup; |
| VPN klient pro neomezený počet přistupujících zařízení součástí nabídky |
| Podpora funkce SSL inspekce (MITM) včetně podpory TLS 1.3 |
| Antivirový engine musí být vybaven lokální databází vzorků škodlivého kódu a AI/ML enginem pro identifikaci podezřelých či neznámých vzorků |
| Funkce ochrany před škodlivým kódem s databází vzorků škodlivého kódu pravidelně aktualizovanou výrobcem, podpora rozpoznávání škodlivého kódu určeného pro mobilní zařízení (tzv. mobile malware), detekce komunikace do sítí typu botnet (minimálně na základě IP adres a domén), podpora ochrany před rychle se šířícími kampaněmi škodlivého kódu (tzv. virus outbreak), podpora sanitarizace aktivního obsahu běžných kancelářských dokumentů (odstranění např. skriptů či maker z dokumentu, extrakce obsahu dokumentu do neškodné podoby); podpora napojení na sandboxovací funkce včetně funkce akceptace lokálních signaturových databází generovaných sandboxem, vše bez nutnosti instalace pluginů do prohlížeče. |
| Funkce rozpoznávání populárních sítových aplikací na základě jejich charakteristiky provozu na aplikační vrstvě, podpora min. 4000 aplikací, pravidelná aktualizace signatur aplikací výrobcem, aplikace rozděleny do přehledných kategorií, možnost vytvářet signatury pro vlastní aplikace |
| Možnost definice zakázaných slov pro vyhledávání na internetu |
| Podpora funkce safe search pro populární vyhledávače |
| Funkce kategorizace webových stránek (web filtering) s podporou minimálně 60 kategorií (pracovní zájmy, osobní zájmy, stránky se škodlivým kódem, nově registrované domény atp.), podpora definice časové kvóty, kterou nesmí daný uživatel na dané kategorii za den překročit, výrobcem aktualizovaná a udržovaná databáze, odpovídající pokrytí českého internetu určení zařízení pro subjekt veřejné správy; požadované akce – povolení stránky, logování stránky, brouzdání s proklikem, nutnost autentizace uživatele pro určitou kategorii, možnost definice časových kvót pro uživatele a kategorie webu |
| Podpora kategorizace stremovaných videí a kanálů min. pro platformu Youtube a Vimeo |
| Funkce ochrany před sítovými útoky (IPS) s výrobcem aktualizovanou databází, přednastavenými profily, možností definovat různé profily na různý druh komunikace, možnost vytvářet vlastní signatury, integrovaný anomální filtr a mechanismus kontroly validity vybraných protokolů |
| Možnost blokovat síťový provoz na základě URL, kategorie webové stránky, IP adresy (rozsahu), GeoIP databáze, data a času |
| Funkce ochrany před unikem citlivých dat (Data Leak Prevention), která umí zachytit pokus o odeslaní/upload označeného dokumentu přes internet na základě vodoznaků, popisu regulárním výrazem atp. |
| Podpora dvoufaktorové autentizace pomocí HW nebo mobilních OTP tokenů, součástí plnění musí být 2 tokeny a plně funkční řešení dvoufaktorového OTP ověřování uživatelů pro administrátory a uživatele VPN |
| Obousměrná integrace (min. ve smyslu sdílení informací o odhalených hrozbách a provozně/telemetrický informací) dodávaného firewallu s dalšími instalovanými bezpečnostní prvky (nástroj pro sběr a vyhodnocování logů, nástroj pro centrální správu aktivních prvků) |
| Podpora režimu nasazení v režimu WCCP (WCCP v2) |
| Podpora konfiguračních PAC souborů pro režim nasazení explicitní proxy |
| Podpora ICAP rozhraní pro obousměrnou integraci s externími servery |
| Podpora tunelování provozu pomocí technologie GRE |
| Podpora automaticky aktivovaného bypass režimu v případě přetížení systému a jeho inspekčních funkcí |
| Analýza a zabezpečení DNS dotazů (ochrana před DNS poisoningem), filtrování DNS dotazů na základě kategorizace |
| Možnost filtrovat Java applety, ActiveX prvky, Cookie soubory ve webovém provozu |
| Integrovaná funkce load balancingu (reverzní proxy) s podporou základní algorimtů pro rozklad zátěže (min. round robin, váhování, nejkratší odezva, nejmenší počet aktivních spojení) s detekcí stavu reálných serverů na pozadí, podpora funkce ssl offloading a ssl inspekce pro rozkládaný provoz |
| Příslušenství - kabely a transceivery | Požadujeme dodání 2 ks SFP+ MM (300m), včetně 2m kabelů LC/LC-LC/LC. |
| Záruka, záruční servis a technická podpora | Nárok na nejnovější firmware a aktualizace požadovaných funkcionalit po dobu 60 měsíců |
| Záruka a záruční servis výrobce zařízení v režimu 24x7 on-site, min. 60 měsíců |

# Přístupový přepínač s příslušenstvím typ A

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky.

|  |  |
| --- | --- |
| Parametr | Popis minimální úrovně parametru |
| Základní a výkonnostní specifikace | Třída zařízení: L2+ switch |
| Formát zařízení do racku |
| Velikost zařízení: 1U |
| min. 48x 10/100/1000Mbit metalických portů |
| min. 4x 10Gbit/s SFP+ nezávislých optických portů s volitelným fyzickým rozhraním |
| 10GE interface zpětně kompatibilní s 1Gbit/s transceivery |
| Všechny ethernet porty jsou dostupné zepředu |
| Interní napájecí zdroj |
| Podpora PoE+ dle standardu 802.3at |
| Dostupný výkon pro PoE+ napájení 370W |
| Podpora Energy Efficient Ethernet (802.3az) |
| Celková propustnost přepínače 176 Gb/s |
| Celkový paketový výkon přepínače 98 Mpps |
| Minimálně 12MB paketový buffer |
| Maximální přípustná hloubka přepínače 31 cm |
| Základní funkce a protokoly | Podpora "jumbo rámců" včetně velikosti 9220 Byte |
| Podpora linkové agregace IEEE 802.3ad |
| Konfigurovatelné rozkládání LACP zátěže podle L3 a L4 |
| Minimální počet LACP skupin/linek ve skupině: 8/8 |
| Protokol pro definici šířených VLAN: MVRP |
| Podpora VLAN podle IEEE 802.1Q, minimálně 512 aktivních VLAN |
| IEEE 802.1s - Multiple Spanning Tree |
| STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+) |
| Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED |
| Detekce jednosměrnosti optické linky (např. UDLD) |
| NTP pro IPv4 a IPv6 včetně MD5 autentizace |
| Statické směrování IPv4 a IPv6 |
| IGMP v2 a v3 |
| MLD v1 a v2 |
| Hardware podpora IPv4 a IPv6 ACL |
| ACL definice na základě skupiny fyzických portů |
| ACL aplikovatelný na rozhraní IN včetně virtuálních VLAN |
| BPDU guard a Root guard |
| HW ochrana proti zahlcení (broadcast/multicast/unicast storm) nastavitelná na množství paketů za vteřinu |
| ICMPv4 a ICMPv6 rate-limiting per port |
| Ověřování 802.1X včetně více uživatelů na port, minimálně 32 uživatelů/port |
| Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou) |
| 802.1X s podporou odlišných Preauth VLAN, Fail VLAN a Critical VLAN |
| Dynamické zařazování do VLAN |
| 802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení) |
| Port security - omezení počtu MAC adres na port, statické MAC |
| Ochrana proti opakovaným výpadkům linek (flapování) s možností konfigurace citlivosti a akce při překročení |
| Ochrana control plane (CPU) před útoky typu DoS |
| Podpora IPv4 a IPv6 QoS |
| Minimálně 8 front pro IEEE 802.1p |
| Management | CLI formou 1x USB-C Console Port |
| Konfigurace zařízení v člověku čitelné textové formě |
| Podpora automatických i manuálních snapshotů konfigurace systému |
| USB port pro diagnostiku, přenos konfigurace a firmware |
| Podpora managementu přes IPv4 i IPv6 |
| SSHv2 a SFTP |
| Podpora SNMPv2c a SNMPv3 |
| RMON |
| Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL |
| Lokálně vynucené RBAC na úrovni přepínače |
| Dualní flash image |
| TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů |
| Podpora Syslog over TLS |
| Podpora RADIUS včetně RADIUS CoA (RFC3576) |
| Podpora RADIUS IPSEC |
| Aktivní monitoring dostupnosti RADIUS přednastaveným jménem a heslem |
| Podpora TACACS+ |
| Analýza síťového provozu sFlow podle RFC 3176 |
| Port mirroring (SPAN), alespoň 4 různé obousměrné session |
| Podpora Zero Touch Provisioning (ZTP) |
| REST API pro automatizaci nastavení |
| Automatická konfigurace portu podle připojeného zařízení |
| Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů |
| Záruky a podpora výrobce | Je požadována záruka na hardware s výměnou NBD v délce 60 měsíců. Tato záruka musí být garantovaná výrobcem zařízení. |
| Je požadován nárok na software aktualizace (nové verze programového vybavení) v minimální délce 60 měsíců. |
| Je požadovaná technická podpora výrobce po dobu min. 60 měsíců. |

# Přístupový přepínač s příslušenstvím typ B

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky.

|  |  |
| --- | --- |
| Parametr | Popis minimální úrovně parametru |
| Základní a výkonnostní specifikace | Třída zařízení: L2+ switch |
| Formát zařízení do racku |
| Velikost zařízení: 1U |
| min. 24x 10/100/1000Mbit metalických portů |
| min. 4x 10Gbit/s SFP+ nezávislých optických portů s volitelným fyzickým rozhraním |
| 10GE interface zpětně kompatibilní s 1Gbit/s transceivery |
| Všechny ethernet porty jsou dostupné zepředu |
| Interní napájecí zdroj |
| Podpora PoE+ dle standardu 802.3at |
| Dostupný výkon pro PoE+ napájení 370W |
| Podpora Energy Efficient Ethernet (802.3az) |
| Celková propustnost přepínače 128 Gb/s |
| Celkový paketový výkon přepínače 95 Mpps |
| Minimálně 12MB paketový buffer |
| Maximální přípustná hloubka přepínače 31 cm |
| Základní funkce a protokoly | Podpora "jumbo rámců" včetně velikosti 9220 Byte |
| Podpora linkové agregace IEEE 802.3ad |
| Konfigurovatelné rozkládání LACP zátěže podle L3 a L4 |
| Minimální počet LACP skupin/linek ve skupině: 8/8 |
| Protokol pro definici šířených VLAN: MVRP |
| Podpora VLAN podle IEEE 802.1Q, minimálně 512 aktivních VLAN |
| IEEE 802.1s - Multiple Spanning Tree |
| STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+) |
| Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED |
| Detekce jednosměrnosti optické linky (např. UDLD) |
| NTP pro IPv4 a IPv6 včetně MD5 autentizace |
| Statické směrování IPv4 a IPv6 |
| IGMP v2 a v3 |
| MLD v1 a v2 |
| Hardware podpora IPv4 a IPv6 ACL |
| ACL definice na základě skupiny fyzických portů |
| ACL aplikovatelný na rozhraní IN včetně virtuálních VLAN |
| BPDU guard a Root guard |
| HW ochrana proti zahlcení (broadcast/multicast/unicast storm) nastavitelná na množství paketů za vteřinu |
| ICMPv4 a ICMPv6 rate-limiting per port |
| Ověřování 802.1X včetně více uživatelů na port, minimálně 32 uživatelů/port |
| Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou) |
| 802.1X s podporou odlišných Preauth VLAN, Fail VLAN a Critical VLAN |
| Dynamické zařazování do VLAN |
| 802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení) |
| Port security - omezení počtu MAC adres na port, statické MAC |
| Ochrana proti opakovaným výpadkům linek (flapování) s možností konfigurace citlivosti a akce při překročení |
| Ochrana control plane (CPU) před útoky typu DoS |
| Podpora IPv4 a IPv6 QoS |
| Minimálně 8 front pro IEEE 802.1p |
| Management | CLI formou 1x USB-C Console Port |
| Konfigurace zařízení v člověku čitelné textové formě |
| Podpora automatických i manuálních snapshotů konfigurace systému |
| USB port pro diagnostiku, přenos konfigurace a firmware |
| Podpora managementu přes IPv4 i IPv6 |
| SSHv2 a SFTP |
| Podpora SNMPv2c a SNMPv3 |
| RMON |
| Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL |
| Lokálně vynucené RBAC na úrovni přepínače |
| Dualní flash image |
| TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů |
| Podpora Syslog over TLS |
| Podpora RADIUS včetně RADIUS CoA (RFC3576) |
| Podpora RADIUS IPSEC |
| Aktivní monitoring dostupnosti RADIUS přednastaveným jménem a heslem |
| Podpora TACACS+ |
| Analýza síťového provozu sFlow podle RFC 3176 |
| Port mirroring (SPAN), alespoň 4 různé obousměrné session |
| Podpora Zero Touch Provisioning (ZTP) |
| REST API pro automatizaci nastavení |
| Automatická konfigurace portu podle připojeného zařízení |
| Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů |
| Záruky a podpora výrobce | Je požadována záruka na hardware s výměnou NBD v délce 60 měsíců. Tato záruka musí být garantovaná výrobcem zařízení. |
| Je požadován nárok na software aktualizace (nové verze programového vybavení) v minimální délce 60 měsíců. |
| Je požadovaná technická podpora výrobce po dobu min. 60 měsíců. |

# Přístupový přepínač s příslušenstvím typ C

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky.

|  |  |
| --- | --- |
| Parametr | Popis minimální úrovně parametru |
| Základní a výkonnostní specifikace | Třída zařízení: L2+ switch |
| Formát zařízení do racku |
| Velikost zařízení: 1U |
| min. 12x 10/100/1000Mbit metalických portů |
| min. 2x 10Gbit/s SFP+ nezávislých optických portů s volitelným fyzickým rozhraním |
| 10GE interface zpětně kompatibilní s 1Gbit/s transceivery |
| Všechny ethernet porty jsou dostupné zepředu |
| Interní napájecí zdroj |
| Podpora PoE+ dle standardu 802.3at |
| Dostupný výkon pro PoE+ napájení 139W |
| Podpora Energy Efficient Ethernet (802.3az) |
| Celková propustnost přepínače 68 Gb/s |
| Celkový paketový výkon přepínače 45 Mpps |
| Minimálně 12MB paketový buffer |
| Bez ventilátoru (fanless) |
| Maximální přípustná hloubka přepínače 31 cm |
| Základní funkce a protokoly | Podpora "jumbo rámců" včetně velikosti 9220 Byte |
| Podpora linkové agregace IEEE 802.3ad |
| Konfigurovatelné rozkládání LACP zátěže podle L3 a L4 |
| Minimální počet LACP skupin/linek ve skupině: 8/8 |
| Protokol pro definici šířených VLAN: MVRP |
| Podpora VLAN podle IEEE 802.1Q, minimálně 512 aktivních VLAN |
| IEEE 802.1s - Multiple Spanning Tree |
| STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+) |
| Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED |
| Detekce jednosměrnosti optické linky (např. UDLD) |
| NTP pro IPv4 a IPv6 včetně MD5 autentizace |
| Statické směrování IPv4 a IPv6 |
| IGMP v2 a v3 |
| MLD v1 a v2 |
| Hardware podpora IPv4 a IPv6 ACL |
| ACL definice na základě skupiny fyzických portů |
| ACL aplikovatelný na rozhraní IN včetně virtuálních VLAN |
| BPDU guard a Root guard |
| HW ochrana proti zahlcení (broadcast/multicast/unicast storm) nastavitelná na množství paketů za vteřinu |
| ICMPv4 a ICMPv6 rate-limiting per port |
| Ověřování 802.1X včetně více uživatelů na port, minimálně 32 uživatelů/port |
| Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou) |
| 802.1X s podporou odlišných Preauth VLAN, Fail VLAN a Critical VLAN |
| Dynamické zařazování do VLAN |
| 802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení) |
| Port security - omezení počtu MAC adres na port, statické MAC |
| Ochrana proti opakovaným výpadkům linek (flapování) s možností konfigurace citlivosti a akce při překročení |
| Ochrana control plane (CPU) před útoky typu DoS |
| Podpora IPv4 a IPv6 QoS |
| Minimálně 8 front pro IEEE 802.1p |
| Management | CLI formou 1x USB-C Console Port |
| Konfigurace zařízení v člověku čitelné textové formě |
| Podpora automatických i manuálních snapshotů konfigurace systému |
| USB port pro diagnostiku, přenos konfigurace a firmware |
| Podpora managementu přes IPv4 i IPv6 |
| SSHv2 a SFTP |
| Podpora SNMPv2c a SNMPv3 |
| RMON |
| Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL |
| Lokálně vynucené RBAC na úrovni přepínače |
| Dualní flash image |
| TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů |
| Podpora Syslog over TLS |
| Podpora RADIUS včetně RADIUS CoA (RFC3576) |
| Podpora RADIUS IPSEC |
| Aktivní monitoring dostupnosti RADIUS přednastaveným jménem a heslem |
| Podpora TACACS+ |
| Analýza síťového provozu sFlow podle RFC 3176 |
| Port mirroring (SPAN), alespoň 4 různé obousměrné session |
| Podpora Zero Touch Provisioning (ZTP) |
| REST API pro automatizaci nastavení |
| Automatická konfigurace portu podle připojeného zařízení |
| Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů |
| Záruky a podpora výrobce | Je požadována záruka na hardware s výměnou NBD v délce 60 měsíců. Tato záruka musí být garantovaná výrobcem zařízení. |
| Je požadován nárok na software aktualizace (nové verze programového vybavení) v minimální délce 60 měsíců. |
| Je požadovaná technická podpora výrobce po dobu min. 60 měsíců. |

## Příslušenství přístupových přepínačů

Pro všechny dodávané přístupové přepínače požadujeme následující celkový počet příslušenství v podobě SFP modulů a kabelů:

* 22 ks SFP+ MM, včetně 2m propojovacích kabelů LC/LC-LC/LC
* 20 ks SFP+ SM, včetně 2m propojovacích kabelů LC/LC-LC/LC

Cena příslušenství musí být zohledněna v ceně samotných přepínačů.

# Licence SW centrálního managementu + 802.1X

|  |  |
| --- | --- |
| Parametr | Popis minimální úrovně parametru |
| Správa a dohled sítě | Požadujeme unifikovaný nástroj pro řešení dohledu a správy sítě pro veškeré nabízené síťové prvky, drátové tak i bezdrátové. |
| Ucelený dohledový a management nástroj správy musí být stejného výrobce jako jsou dodávané síťové prvky. |
| Musí obsahovat konfiguračním workflow, umožňující jednoduché nasazení a nastavení síťového prostředí, zejména složitějších scénářů, jako např. zavedení 802.1x. |
| Musí umožnit hromadnou konfiguraci i výstupy skrze CLI spravovaných přepínačů |
| Nástroj musí podporovat „Zero Touch Provisioning“ dodávaných prvků |
| Nástroj musí disponovat přehledy, reporty i celkovou kontrolou zdraví jednotlivých prvků sítě či celé lokace. |
| Nástroj bude zabezpečovat automatizované sledování, plánování a nasazování aktuálních verzí firmware tak, aby byl zabezpečen dlouhodobý, bezpečný a hladký provoz, včetně odstraňování případných chyb či rozšiřování palety funkcí firmware. Musí umožnit správu životního cyklu zařízení. |
| Požadujeme napojení (integraci) na centrální logovací systém |
| Řízení přístupu k síti | Nástroj bude umožňovat sestavit a použít profily pro řízení přístupu k síti, sjednocené pro drátovou i bezdrátovou síť. |
| Požadujeme přímé napojení na používané centrální identitní služby – Microsoft Active Directory nebo Azure Active Directory za účelem centrálního řízení přístupu k síti na bázi identity. |
| Požadujeme ve WiFi síti oddělení uživatelů/zařízení na bázi jedinečného klíče (PSK) bez nutnosti vytvářet další oddělné SSID. |
| Požadujeme nástroj pro snadné zavedení nového zařízení, ideálně formou jednoduché aplikace nebo web. portálu pro nejpoužívanější operační systémy (iOS, Android, Windows 10+). |
| Autentizační proces | Požadujeme vyšší úroveň správy i autentizačního procesu pomocí vlastní inteligence zabudované v nástroji (AI/ML apod.). |
| Diagnostické přehledy tzv. Insights a případná doporučení změn pro lepší uživatelskou zkušenost či funkci dodávaného řešení jako celku |
| Guest portál – požadujeme upravitelný (konfigurovatelný) portál k řízení přístupu hosta s podporou autentizace pomocí tzv. „Social ID“ (Facebook, Google, Linkedin, apod.). |
| Záruky a podpora výrobce | Je požadován nárok na software aktualizace (nové verze programového vybavení) v minimální délce 60 měsíců. |
| Je požadovaná technická podpora výrobce po dobu min. 60 měsíců. |

# Přístupové wifi body s příslušenstvím

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky.

|  |  |
| --- | --- |
| Parametr | Popis minimální úrovně parametru |
| Základní požadavky | Třída zařízení: Indoor přístupový bod |
| Minimální počet portů ethernet LAN: 1x 100/1000 Mbit/s RJ45 |
| Podpora bezdrátových standardů: 802.11a/b/g/n, 802.11ac wave2, 802.11ax |
| Certifikace Wi-Fi Aliance: Wi-Fi CERTIFIED 6™ a Wi-Fi CERTIFIED WPA3™ |
| Plnohodnotná certifikace Wi-Fi Aliance: IEEE 802.11a/b/g/n/ac |
| Radiová část: dual band, současná podpora pásem 2,4GHz a 5GHz |
| MIMO a počet nezávislých streamů na 2,4GHz rádio: 2x2:2 |
| MIMO a počet nezávislých streamů na 5GHz rádio: 2x2:2 |
| Výkonová specifikace | Minimální komunikační rychlost na fyzické vrstvě (Max data rate) pro 5GHz: 1200 Mbps |
| Minimální komunikační rychlost na fyzické vrstvě (Max data rate) pro 2.4GHz: 570 Mbps |
| Hardware filtry pro filtraci intermodulačního rušením pocházejícím z mobilních sítí (Advanced Cellular Coexistence nebo obdobné) |
| Možnost nastavení vysílacího výkonu s krokem 0.5 dBm |
| Podpora standardního PoE IEEE 802.3af 15W bez nutnosti redukce výkonu libovolného rádia |
| Funkční specifikace | Pracovní režim AP bez kontroléru (autonomní) |
| Pracovní režim AP řízené kontrolérem (lightweight) |
| Pracovní režim AP v roli kontroléru s možností správy až 120 AP |
| Automatické ladění kanálu a síly signálu v koordinaci s ostatními AP |
| Integrovaný TPM pro bezpečné uložení certifikátů a klíčů |
| Podpora 802.11ac explicitního beamformingu |
| Podpora airtime fairness |
| Prioritizace jednotlivých SSID na základě vysílacího času |
| Band Steering či obdobné (prioritizace 5GHz pásma v případě je-li podporováno) |
| Detekce Rogue AP |
| Minimální počet inzerovaných SSID (BSSID) na radio: 16 |
| Mapování SSID do různých VLAN podle IEEE 802.1Q |
| Podpora Layer-2 izolace bezdrátových klientů |
| Automatická identifikace připojeného zařízení a jeho operačního systému |
| Předávání konektivity mezi AP při pohybu bez výpadku spojení – roaming |
| Dynamické vyvažování zátěže klientů mezi AP se zohledněním zátěže, počtu klientů, síly signálu v koordinaci s ostatními AP |
| Optimalizace provozu: multicast-to-unicast konverze |
| Možnost řízení QoS (šířky pásma) na základě aplikací (Office 365, Dropbox, Facebook, P2P sdílení, VoIP, video aplikace) |
| Filtrování přístupu na web |
| Podpora MAC ověřování a 802.1X ověřování s využitím lokální DB v AP |
| Podpora 802.1X suplicant, AP se ověřuje před připojením do LAN |
| Volitelně možnost spravovat AP cloud management nástrojem |
| CLI formou serial konsole port a serial over bluetooth |
| SSHv2, SNMPv2c a SNMPv3 |
| Součástí AP je příslušenství pro montáž na strop |
| AP podporuje zero touch provisioning pomocí externího management SW jehož IP adresu získá z cloud aktivační služby poskytované výrobcem |
| Záruka, záruční servis a technická podpora | Je požadována záruka na hardware s výměnou NBD v délce 60 měsíců. Tato záruka musí být garantovaná výrobcem zařízení |

# Záložní zdroj pro aktivní prvky s příslušenstvím

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky.

| Parametr | Popis minimální úrovně parametru |
| --- | --- |
| Základní požadavky | Záložní zdroj napájení (UPS) |
| Desktopová- samostatně stojící UPS (věžový typ) |
| Maximální hloubka 45 cm |
| Typ použitých baterií - bezúdržbové, hermeticky uzavřené, ventilem řízené olověné baterie |
| Výkonové požadavky | Parametry vstupního napětí - 220/230/240 V, 40 -70 Hz |
| Parametry výstupního napětí - 220/230/240 V (volitelné), 50 Hz/60 Hz (volitelné) |
| Max. nastavitelný výkon 600 W |
| Jmenovitý výkon 1 000 VA |
| Funkční požadavky | Topologie – Standby |
| Přípojky:   * min. 8x IEC 320 C13 |
| Přední ovládací panel s LCD, s akustickým a vizuálním varováním |
| Podpora síťového monitoringu (min. informace o stavu nabití baterií a informace o stavu baterií) |
| Podpora připojení k PC pomocí USB kabelu |
| Požadavky na záruku a prodlouženou záruku | Záruka na UPS jako celek s výjimkou baterie min. 60 měsíců |
| Záruka na baterie min. 24 měsíců |

# Nástroj pro logování infrastruktury

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky.

|  |  |
| --- | --- |
| Parametr | Popis minimální úrovně parametru |
| Minimální HW parametry požadovaného systému | Jedna hardwarová appliance o velikosti max. 1U, včetně ramena pro kabelový management umožňujícího vysunutí zapnutého systému z racku pro servisní účely. |
| HW appliance obsahuje veškeré potřebné komponenty (CPU, RAM, diskový prostor) pro svoji činnost a je nezávislá na dalších systémech. |
| Řadič diskového pole musí obsahovat zálohovací baterii nebo být vybaven flash pamětí. |
| Z výkonových důvodů požadujeme, aby v systému byly minimálně 4 ks stejných RAID edition disků určených pro použití v datacentrech, o rychlosti minimálně 7200 otáček/m. |
| Minimálně 4x 1Gbit LAN porty + 1x dedikovaný 1Gbit port pro management HW. Konfigurace všech parametrů síťového rozhraní včetně link agregace dle LACP (802.3ad), VLAN a IP adresace v jednotném webovém rozhraní systému a doložte příslušný odkaz na dokumentaci. |
| Větráky v systému musí být vyměnitelné za provozu a redundantní. |
| 2x napájecí zdroje s redundancí napájení 1+1. |
| Virtuální KVM (tj. převzetí textové i grafické konzole serveru a zajištění přenosu povelů z klávesnice a myši vzdáleného počítače. |
| Systém pro vzdálenou správu serveru včetně potřebné licence, pokud je třeba (obdoba HP iLO, Dell iDRAC apod). |
|  |  |
| Výkonnostní a SW parametry systému | Systém funguje formou HW appliance (všechny části systémů je možné nastavit v centrální webové konzoli a není nutné editovat žádné konfigurační soubory, scripty nebo makra v příkazové řádce). |
| Aktualizace systému a jejich instalace bude prováděna uživatelsky přes centrální webovou správcovskou konzoli. Všechny aktualizace musí být prováděny z webového prostředí bez potřeby asistence dodavatele/výrobce dodávaného systému. |
| Systém musí podporovat downgrade v jednom kroku, pro případ problémů s novou verzí systému po upgrade. Není přípustný downgrade pouze za součinnosti výrobce. |
| Průměrný trvalý příjem min. 2000 událostí/s. Výkon musí být dosažen na požadované množství událostí s průměrnou délkou zpráv minimálně 700Byte trvale. Systém musí prokazatelně kompletně zpracovat přijaté události včetně vytváření očekávaných metadat (DNS-PTR, čísla a jména ASN, geolokace), zajišťovat normalizaci, zamezovat ztrátě přijatých událostí nebo posunutí důvěryhodného časového razítka oproti času skutečného příjmu každé události. |
| Špičkový příjem minimálně 4000 událostí/s po dobu nejméně 10 minut a průměrnou délkou minimálně 700byte. Systém musí prokazatelně kompletně zpracovat přijaté události, zamezovat ztrátě ukládaných dat nebo posunutí důvěryhodného časového razítka oproti času skutečného příjmu zpráv. Při zpracování dat během špičkového příjmu akceptujeme zpoždění zobrazení zpracovávaných dat. Systém ani ve špičkovém výkonu nesmí dovolit ztrátu dat, skluz důvěryhodného časového razítka nebo jiné prokazatelné vady na zpracovávaných datech oproti zpracování při průměrném trvalému příjmu událostí.  V případě krátkodobého (do 10 minut) až dvounásobného přetížení systému proti jeho tabulkovým hodnotám nesmí dojít ke ztrátě logů nebo nesprávnému stanovení časového razítka. Všechny přijaté nezpracované logy/události musí být ukládány do vyrovnávací paměti. |
| Licenčně neomezený počet zařízení pro příjem zasílaných událostí. Licenčně neomezený počet událostí v GB za den nebo licence na minimálně 200GB uložených událostí za den. Integrovaná databáze musí mít čistou velikost (kapacitu) nejméně 12 TB a nad to musí podporovat kompresi ukládaných dat. |
| Požadujeme uživatelskou konfiguraci klasifikace dat, parserů, filtrů a alertů, prováděnou pomocí vizuálního programovacího jazyka v centrální správcovské webové konzoli. Vizuální programovací jazyk musí uživateli umožnit psát konfigurace bez nutnosti znalosti programování (např. Node-RED, Microsoft VPL, Blockly apod). |
| Konfigurace uživatelských parserů musí umožňovat automatické doplňování DNS reverzních záznamů, čísel a jmen autonomních sítí, geolokační informace a identifikace výrobce zařízení podle MAC adresy. |
| Systém musí podporovat doplňování zpráv o informace z textových prohledávacích tabulek. (Například k uživatelskému jménu doplnit z textové prohledávací tabulky informaci o jeho emailu, členství v AD skupinách a podobně). Pro automatickou aktualizaci takto uložených doplňujících informací musejí být tyto textové prohledávací tabulky naplnitelné pomocí REST API nabízeného systému a modifikovatelné přes jednotné webové rozhraní. |
| Možnost on-line ladění uživatelsky definovaných parserů - při jejich vytváření je možné vložit skupinu testovacích zpráv, při změně je okamžitě zobrazena výsledná podoba rozparsovaných dat a případná chybová hlášení s upozorněním na chybná místa vytvářeného parseru. Pro snadnější vytváření parserů požadujeme mít možnost vložení minimálně 20 testovacích zpráv současně. |
| V centrální správcovské konzoli je možné přidávat k jednotlivým zdrojům dat, aplikacím, zařízením nebo IP subnetům tzv. značky, označující například umístění zařízení, typ zařízení, kritičnost zařízení apod. Systém obsahuje předdefinované značky, které automaticky přidává k přijímaným zprávám. Zejména následující značky: konfigurační změna, úspěšné ověření uživatele, neúspěšné ověření uživatele, zpráva přišla z windows, zpráva byla vygenerována firewallem |
| Všechny přidávané značky budou ukládány s každou přijatou událostí, na základě značky bude možné filtrovat data nebo omezovat oprávnění uživatelů systému k jednotlivým událostem. |
| Systém musí umožňovat export dat ve formátu vhodném pro další strojové zpracování bez dodatečných omezení na časové období, množství nebo obsah exportovaných dat. Během exportu je možné označit pouze vybraná pole, která mají být do exportu zahrnuta. |
| Podpora zálohování nebo obnovení konfigurace v jednom kroku a jednom souboru pro celý systém. |
| Podpora důvěryhodného zálohování dat na externí systém. Požadováno plánované i ad-hoc zálohování. Zálohy dat musejí být vhodně kompresovány a umožnit v budoucnosti obnovení bez ohledu na verzi systému, ve které byla záloha pořízena. |
|  |  |
| Obecné požadavky na systém pro centralizovanou správu logů, událostí a strojových dat | Požadujeme systém, který pracuje jako hardwarová appliance s jedním uceleným webovým rozhraním pro všechny administrátorské i operátorské činnosti. Nevyžaduje instalaci dalších systémů a aplikací, vyjma agenta pro sběr Windows logů. Doložte katalogový list produktu (datasheet) podrobně popisující hardwarové i softwarové parametry nabízeného systému. |
| Systém musí zpracovávat události z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware používaného u zadavatele nebo pořizovaného v rámci tohoto plnění (současně používané servery a úložiště HPE, síťové prvky HPE a Fortinet). |
| Veškerá konfigurace systému se musí provádět v grafickém rozhraní jednotné uživatelské webové konzole. Systém bude poskytovat podporu pro vizuální programování pro všechny kroky zpracování strojových dat. |
| Systém musí umožňovat dopsání parserů pro další (výše neuvedená) zařízení uživatelem bez nutnosti spolupráce s výrobcem nebo dodavatelem (vč. subdodavatelů) nabízeného systému - Uživatelsky definované parsery. Dokumentace musí obsahovat přehledný návod na vytváření zákaznických parserů a systém musí obsahovat možnost testování a ladění zákaznických parserů v jednotném ovládacím grafickém webovém rozhraní. Vytváření a testování parserů nesmí mít vliv na provoz systému. Pro psaní parserů nesmí být použito textové psaní programového kódu ale tzv. vizuální programování, které automaticky opravuje uživatele a upozorňuje ho na chyby. |
| Systém umožňuje v grafickém rozhraní vizuálního programovacího jazyka snadno provádět třídění a značkování vstupních dat pro jejich další zpracování. Nepřipouští se nastavování třídění vstupních dat ve formě skriptu/makra zobrazeného v textovém okně. |
| Systém bude přijímat a zpracovávat logy, události a další strojově generovaná data prostřednictvím minimálně následujících protokolů: SYSLOG (dle RFC3164, RFC5424, RFC5425) a RELP. Systém musí umožňovat příjem logů i na rozsahu alespoň 50 UDP a TCP portů pro zjednodušené třídění vstupních zpráv. Dále požadujeme podporu sběru strojových dat z databází s nastavením v grafickém menu systému minimálně pro databáze MSSQL, MySQL a PostgreSQL a to bez nutnosti instalovat na databázový server doplňkový software nebo agenta. |
| Přijaté logy bude systém standardizovat do jednotného formátu a logy budou normalizovány (rozdělovány) do příslušných polí dle jejich typu. Zároveň systém bude uchovávat i originální verzi zpráv. Integrované parsery systému budou automaticky přidávat ke zprávám, kterých se to týká, meta informace o jaký druh zprávy se jedná, minimálně požadujeme rozlišení těchto druhů zpráv: úspěšné přihlášení, neúspěšné přihlášení, odhlášení, konfigurační změna, značka/tag. Tyto meta informace musí být možné přidávat i v uživatelsky definovaných parserech. |
| Hodnoty jednotlivých parsovaných polí bude možné v definici parseru přetypovat a standardizovat alespoň na tyto základní druhy: číslo, IP adresa, MAC adresa, URL. Nad uloženými čísly je pak bude možné při prohledávání dat provádět matematické operace (součty všech hodnot, průměry, nejmenší/největší hodnota apod.). |
| Všechna pole a položky přijaté systémem budou automaticky indexovány tak, aby nad všemi položkami bylo možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem. |
| Možnost sběru událostí minimálně ve formátech RAW, Syslog RFC5424, CEF, LEEF, JSON RFC8259. |
| Systém nesmí v žádném případě umožnit mazání nebo modifikování již uložených logů v rámci požadované retence. A to ani libovolnou konfigurační změnou - administrátorovi s nejvyššími oprávněními k navrhovanému systému. Každý zpracovaný log musí mít dohledatelný unikátní identifikátor, který umožní jeho jednoznačnou identifikaci. |
| Systém bude umožňovat snadné vyhledávání událostí a okamžité vytváření grafických reportů (ad hoc) bez nutnosti dodatečného programování nebo aplikování dotazů v SQL jazyce. Reportovací nástroj musí být integrální součástí navrhovaného systému a musí se obsluhovat v jednotném rozhraní nabízeného produktu. |
| Systém bude provádět ucelenou vizualizaci logů, událostí a strojových dat (grafy událostí). Vizualizace musí být dynamická, tj. volbou v jednom grafu se ostatní příslušné grafy v pohledu na data upraví dle požadované volby automaticky. |
| Systém bude umožňovat snadné vytváření grafických znázornění událostí v dashboardech nad všemi uloženými daty za libovolné časové období bez nutnosti nejprve modifikovat konfiguraci systému nebo parametrů uložených dat. Historická data v požadované délce retence uložená v systému bude možné prohledávat okamžitě bez časových prodlev opětovného importu nebo dekomprimace starších dat, prohledávání dat nesmí vyžadovat manuální konfiguraci a zásahy uživatele. |
| Systém musí podporovat nativní získávání logů z Office365/Microsoft365 prostředí bez ohledu na použitou licenci 365 prostředí a bez nutnosti instalovat dodatečné externí komponenty. Město Kaplice provozuje Microsoft365. Požadujeme předložit link na dokumentaci popisující nastavení systému v jednotném grafickém rozhraní tak, aby získával logy z Office365/Mircosoft365. |
| Systém musí umožňovat unifikované vyhledávání napříč všemi typy dat a zařízeními dle normalizovaných polí (uživatelské jméno, zdrojová IP, značka/tag apod.). |
| Dodavatel musí předložit potvrzení vystavené autorizovanou osobou o shodě, že nabízený systém splňuje požadavky normy ČSN/ISO 27001:2013 na pořizování auditních záznamů, nebo jiné normy obdobné nebo stejné úrovně v prostředí evropského hospodářského prostoru (EHP). Toto potvrzení není možné nahradit certifikátem na společnost dodavatele (subdodavatele) nebo výrobce nabízeného systému. Nelze nahradit čestným prohlášením. |
| Systém musí mít možnost uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování. Továrně dodané pohledy na data nesmí jít uživatelem systému nevratně modifikovat nebo smazat. |
| Systém bude obsahovat předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění. |
| Konfigurační a Systémové rozhraní a dokumentace k těmto rozhraním musí být identické v anglickém i v českém jazyce. Nepřipouští se omezená dokumentace v českém jazyce nebo zjednodušená dokumentace odkazující na další dokumentaci v anglickém jazyce, případně na dokumentaci třetích stran. |
| Čistá kapacita úložného prostoru (kapacita diskového pole) dostupná pro uložená data nabízeného systému musí být minimálně 12TB. |
| Monitoring stavu systému - alertování při překročení prahových hodnot nebo chybě systému, přeposlání upozornění pomocí SMTP nebo Syslog. |
| Požadujeme, aby systém obsahoval REST-API pro integraci s externím monitorovacím systémem (zejména Zabbix, PRTG a další) a umožňoval autorizovaný přístup ke strukturované databázi logů. |
| Dodavatel doloží prohlášení výrobce o shodě s požadavky Vyhlášky 82 / 2018 Sb. „o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)“ k Zákonu 181 / 2014 Sb. „o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).“ |
| Požadujeme jednotnou centrální webovou konzoli s jednotným grafickým rozhraním pro přístup k logům, alertům, reportům a pro správu systému. Z této konzole se provádí veškerá konfigurace, správa i analýza logů. Není přípustné, aby navrhovaný systém měl více rozdílných konzolí od různých výrobců s rozdílným ovládáním nebo aby se konfigurace musela provádět mimo jednotné webové rozhraní. |
| Požadujeme, aby systém umožňoval jednotné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem na základě typu zdrojů a značek a k jednotlivým ovládacím komponentům systému. |
| Dodaný systém musí obsahovat ucelené all-in-one řešení pro parsování a normalizaci přijatých událostí bez nutnosti dodatečné instalace externích aplikací nebo systémů. Jedinou přípustnou výjimkou je monitorování systémů Windows pomocí agentů. |
| Systém musí podporovat ověřování uživatele systému na externím LDAP serveru. V případě výpadku externího LDAP systému musí podporovat ověření lokálního účtu. Systém automaticky zaznamenává uživatelská jména u akcí provedených konkrétním uživatelem. |
|  |  |
| Alerty | Požadujeme aby systém byl schopen na základě uživatelsky zadaných podmínek splněných v přijatých datech vygenerovat alert. |
| Text emailu vygenerovaného alertem musí být uživatelsky definovatelný s proměnnými, které jsou vyplněny z přijaté rozparsované události. |
| Systém musí obsahovat výrobcem předpřipravené sety/vzory alertů a korelací. |
| Systém musí provádět konfigurace alertů a korelací pomocí vizuálního programovacího jazyka. Vizuální programovací jazyk není prezentován čistě textově, ale textově-grafickou formou, která vizualizuje aplikační logiku vytvářeného alertu. Konfigurace alertů musí umožňovat okamžitou kontrolu funkčnosti výstupu alertu nebo korelace vložením příslušné testovací zprávy, včetně zobrazení upozornění na případné uživatelské chyby. |
| Jako výstupní pravidlo Alertu musí systém umět odeslat událost, která alert vyvolala, na externí systém minimálně prostřednictvím SMTP nebo Syslogu přes TCP protokol. U Syslog protokolu požadujeme možnost definice formátu odesílaných dat pro snazší integraci se systémy třetích stran. |
| V alertech je možné nejen využívat, ale i přiřazovat značky (zejména: pošli alert jen v případě, že se událost stala na kritickém serveru a je označen názvem lokality, nebo pokud událost obsahuje podmínku, přiřaď novou značku). |
| Požadujeme, aby systém podporoval základní funkce SIEM - funkce pro korelace událostí a upozornění s hraničními limity. Definice korelačních pravidel bude prováděna pomocí vizuálního programovacího jazyka a musí obsahovat možnost vložení testovací zprávy a zobrazení výsledku testu o provedené akci. |
|  |  |
| Sběr událostí z Microsoft prostředí | Windows agent nevyžaduje administrátorské zásahy na koncovém systému – je centrálně spravovaný a jeho konfigurace musí být kompletně realizována v grafickém rozhraní systému bez využití skriptů nebo maker. Konfigurace musí být automaticky distribuována přímo z centrální konzole systému.Tj. vlastní správa a aktualizace Windows agenta se neprovádí z Group Policy. |
| Komunikace Windows agenta a centrálního systému musí být zabezpečena min. na úrovni TLS 1.2 a výše a musí podporovat ověřování certifikátem. |
| Windows agent podporuje sběr nejen ze základních systémových logů (Aplikace, Zabezpečení, Instalace, Systém), ale je možné z centrální konzole v grafickém rozhraní nastavit i sběr všech ostatních logů ve složce Protokoly aplikací a služeb a logy rozšířené Sysmonem. Dále musí Windows agent podporovat centralizované nastavení z administrátorské konzole systému pro sběr textových logů včetně možnosti výběru jejich formátu. |
| Windows agent automaticky doplňuje ke všem odesílaným událostem jejich textový popis tak, jak je zobrazen v Prohlížeči událostí (Event Viewer) na koncovém systému. |
| Počet instalací Windows agenta požadujeme bez licenčního a časového omezení, v případě že to pro nabízené řešení není možné, tak požadujeme dodání licencí na Windows agenty v množství 500 ks na dobu předpokládané morální životnosti produktu – 7 let. Předpokládáme instalaci agentů na všechny systémy současně, proto je nutné potvrdit, zda systém výkonnostně splňuje tento požadavek. |
|  |  |
| SW Podpora a záruka na hardware | HW - Požadovaná min. 5letá servisní podpora na hardware appliance s opravou v místě instalace a s garantovanou odezvou následující pracovní den od nahlášení případné závady. |
| Systém musí podporovat vygenerování TSR (technického support reportu) pro možnost diagnostiky bez vzdáleného přístupu. |
| SW - Podpora výrobce na aktualizaci systému a parserů na 5 let. Podpora musí obsahovat aktualizaci SW, opravy chyb a telefonickou a emailovou podporu s diagnostikou vzdáleným přístupem. |

# Produkční servery s příslušenstvím

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky.

| Parametr | Popis minimální úrovně parametru |
| --- | --- |
| Základní a výkonové požadavky | **Typ zařízení -** Šasi pro montáž do standardního racku o velikosti max. 2U. Požadujeme dodání serveru s rackmount příslušenstvím včetně pohyblivého ramene pro zachycení kabeláže |
| **Procesor -** CPU - architektura x86 s 16 plnohodnotnými jádry. V testu na cpubenchmark.net minimálně 40 000 bodů. Max. počet CPU je omezen na 1 a počet jader je omezen na 16 core z důvodu licencování OS a aplikací. |
| **Paměť**   * 512GB, min. typu DDR4 s taktem 3200MT/s, Dual Rank |
| **Pevné disky**   * Server musí být osaditelný min. 24x disky NVMe SSD a 2 disky na instalaci OS. Veškeré potřebné komponenty (řadič, diskové pozice, kabeláž, napájecí zdroje apod.) musí být součástí dodávky tak, aby server bylo možné funkčně osadit plným počtem SSD pouhým dodatečným vložením disků * Požadujeme dodat 2 ks disků min. 1.6TB, NVMe, High Performance, Mixed Use, DWPD3 a 8 ks disků min. 3.84TB, NVMe, Mainstream Performance, Read Intensive, DWPD1 |
| **OS Boot**   * Musí být zajištěn dvojicí disků v RAID1 a kapacitou min. 240GB, nesmí se jednat o rotační disky * Disky musí být připojeny na jiný RAID řadič, než datové disky |
| **LAN konektivita**   * min. 2 ks Ethernet adapter Dual Port 10/25GbE Adapter (RoCE v2, DCB, RDMA) včetně 2 ks SM zářičů 25G a 2m kabelů LC/LC-LC/LC a 2 ks MM SFP+ zářičů včetně 2m kabelů LC/LC-LC/LC. Karty budou od stejného výrobce se stejnou produktovou řadou, je požadována plná kompatibilita s virtualizační platformou VMware – vSAN. * min. 1ks Ethernet adapter 2x 1GbE 1000BASE-T |
| **Napájení a chlazení**   * Server musí být vybaven redundantním napájením a chlazením, hot-plug vyměnitelné za provozu * 2ks hot-swap zdroje napájení dimenzované pro plné osazení serveru disky, CPU, RAM a PCIe zařízení, účinnost min. 96% |
| Funkční požadavky | Server musí být osazen TPM 2.0 |
| Vyčítání přes SNMP celkového zdraví serveru bez nutnosti instalovat OS – jeden parametr v MIB |
| IPMI 2.0 popř. obdoba, možnost vzdáleného převzetí grafické konsole bez závislosti na OS, webový klient HTML5, vzdálený mount DVD media, USB, dedikovaný port (není součástí požadovaného počtu ethernet portů) |
| Kompatibilita všech komponent s OS VMWARE ESXi 8.x a VSAN 8.x v architektuře OSA (stávající virtualizační platformou zadavatele) dle veřejně dostupného seznamu např.: https://www.vmware.com/resources/compatibility/search.php?deviceCategory=vsanesa |
| Záruka, záruční servis a technická podpora | Je požadována záruka na dobu 5 let s reakční dobou na založený incident na kompletní HW a přístup k technické podpoře 24x7, 4h |
| Servisní zásahy provádí technik s příslušnou znalostí, schválený výrobcem |
| Nárok na aktualizace systému dostupné min. po dobu záruky, nabízené přehledně v servisním portálu po zadání sériového čísla |

# Management server s příslušenstvím

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky.

| Parametr | Popis minimální úrovně parametru |
| --- | --- |
| Základní a výkonové požadavky | **Typ zařízení**   * Šasi pro montáž do standardního racku o velikosti max. 2U. * Požadujeme dodání serveru s rackmount příslušenstvím včetně pohyblivého ramene pro zachycení kabeláže |
| **Procesor -** 1ks CPU - architektura x86 s 16 plnohodnotnými jádry. V testu na cpubenchmark.net minimálně 40 000 bodů. Max. počet CPU je omezen na 1 a počet jader je omezen na 16 core z důvodu licencování OS a aplikací. ~~TDP max. 155W.~~ |
| **Paměť**   * 128GB, min. typu DDR4 s taktem 3200MT/s, Dual Rank |
| **Řadič datového diskového systému - minimální požadované vlastnosti**   * typu SAS, min. x8 PCI Express 3.1 kompatibilní, dvoukanálový (2 konektory) * podpora RAID 0, 1, 10 * podpora 6/12Gbps technologie rozhraní disků, 12Gbps na port * podpora S.M.A.R.T. * podpora globálního i dedikovaného hot-spare |
| **Pevné disky**   * Server musí být osaditelný min. 8x 2,5" disky SATA, SAS HDD a SSD. Veškeré potřebné komponenty (řadič, diskové pozice, kabeláž, napájecí zdroje apod.) musí být součástí dodávky tak, aby server bylo možné funkčně osadit plným počtem HDD pouhým dodatečným vložením disků. * Požadujeme dodání 2 ks disků min. 1.92TB SATA/SAS SSD, DWPD 1, hot-swap |
| **OS Boot**   * Musí být zajištěn dvojicí disků v RAID1 a kapacitou min. 240GB, nesmí se jednat o rotační disky * Disky musí být připojeny na jiný RAID řadič, než datové disky |
| **LAN konektivita**   * min. 1ks Ethernet adapter Dual Port 10/25GbE Adapter (RoCE v2, DCB, RDMA) včetně SFP+ MM zářičů a 2m kabelů LC/LC-LC/LC. Karta bude od stejného výrobce jako u produkčních serverů, které jsou součástí tohoto plnění, je požadována plná kompatibilita. * min. 1ks Ethernet adapter 2x 1GbE 1000BASE-T |
| **Napájení a chlazení**   * Server musí být vybaven redundantním napájením a chlazením, hot-plug vyměnitelné za provozu * 2ks hot-swap zdroje napájení dimenzované pro plné osazení serveru disky, CPU, RAM a PCIe zařízení, účinnost min. 96% |
| Funkční požadavky | Server musí být osazen TPM 2.0 |
| Vyčítání přes SNMP celkového zdraví serveru bez nutnosti instalovat OS – jeden parametr v MIB |
| IPMI 2.0 popř. obdoba, možnost vzdáleného převzetí grafické konsole bez závislosti na OS, webový klient HTML5, vzdálený mount DVD media, USB, dedikovaný port (není součástí požadovaného počtu ethernet portů) |
| Záruka, záruční servis a technická podpora | Je požadována záruka na dobu 5 let s reakční dobou na založený incident na kompletní HW a přístup k technické podpoře 24x7, 4h |
| Servisní zásahy provádí technik s příslušnou znalostí, schválený výrobcem |
| Nárok na aktualizace systému dostupné min. po dobu záruky, nabízené přehledně v servisním portálu po zadání sériového čísla |

# Licence OS produkčních serverů a licence OS BackUp a management serveru

**Je požadována dodávka následujících licencí**

|  |  |
| --- | --- |
| Počet | Typ licence |
| 2 | Windows Server Datacenter 2022 v rozsahu k pokrytí dodaných procesorových core v každém produkčním serveru |
| 2 | Windows Server Standard Core 2022 - 16 Lic Core Lic (BackUp server a management server) |
| 115 | Windows Server CAL 2022 - per User |

Je požadována dodávka licencí, jejichž pravost je garantovaná a ověřitelná u vlastníka autorských práv MICROSOFT. V databázi MICROSOFT musí být kupující veden jako první a jediný uživatel zboží (licencí).

Je připuštěno zpřístupnění instalačních balíčků, produktových klíčů a přehled o zakoupených licencích na www.microsoft.com.

Jsou požadovány licence pro užití On-Premise.

**Zdůvodnění požadavku na kompatibilitu**

Zadavatel provozuje své technologické prostředí postavené na platformě OS Windows a hypervisoru VMware. Na této platformě je pak provozována majorita agendových informačních systémů zadavatele, které slouží k zajištění výkonu jeho veřejné správy a dále k zajištění interních činnosti a agend. Na této platformě jsou rovněž provozována adresářové služby a řízení uživatelských účtů a práv v nich. Z těchto důvodů je požadována kompatibilita s tímto technologickým prostředím a jako definice požadavku je uveden konkrétní produktový název.

# Licence řízení hypervisoru pro management server

|  |  |
| --- | --- |
| Počet | Typ licence |
| 1 | VMware vCenter Server Standard for vSphere |

Pro dodávané servery je požadována dodávka virtualizačního software (hypervisoru) VMware vSphere kompatibilního se stávajícím serverovým virtualizačním prostředím VMware kupujícího k licenčnímu pokrytí všech serverů, které jsou součástí tohoto plnění.

**Zdůvodnění požadavku na kompatibilitu**

Zadavatel provozuje své technologické prostředí postavené na platformě OS Windows a hypervisoru VMware. Na této platformě je pak provozována majorita agendových informačních systémů zadavatele, které slouží k zajištění výkonu jeho veřejné správy a dále k zajištění interních činnosti a agend. Na této platformě jsou rovněž provozována adresářové služby a řízení uživatelských účtů a práv v nich. Z těchto důvodů je požadována kompatibilita s tímto technologickým prostředím a jako definice požadavku je uveden konkrétní produktový název.

# Licence hypervizoru pro produkční servery

|  |  |
| --- | --- |
| Počet | Typ licence |
| 3 | VMware vSphere Standard 1 Processor |

Pro dodávané servery je požadována dodávka virtualizačního software (hypervisoru) VMware vSphere kompatibilního se stávajícím serverovým virtualizačním prostředím VMware kupujícího k licenčnímu pokrytí všech serverů, které jsou součástí tohoto plnění.

**Zdůvodnění požadavku na kompatibilitu**

Zadavatel provozuje své technologické prostředí postavené na platformě OS Windows a hypervisoru VMware. Na této platformě je pak provozována majorita agendových informačních systémů zadavatele, které slouží k zajištění výkonu jeho veřejné správy a dále k zajištění interních činnosti a agend. Na této platformě jsou rovněž provozována adresářové služby a řízení uživatelských účtů a práv v nich. Z těchto důvodů je požadována kompatibilita s tímto technologickým prostředím a jako definice požadavku je uveden konkrétní produktový název.

# Licence SW pro diskovou virtualizaci

|  |  |
| --- | --- |
| Počet | Typ licence |
| 2 | VMware vSAN Standard 1 Processor |

Pro dodávané servery je požadována dodávka virtualizačního software (hypervisoru) VMware vSphere kompatibilního se stávajícím serverovým virtualizačním prostředím VMware kupujícího k licenčnímu pokrytí všech serverů, které jsou součástí tohoto plnění.

**Zdůvodnění požadavku na kompatibilitu**

Zadavatel provozuje své technologické prostředí postavené na platformě OS Windows a hypervisoru VMware. Na této platformě je pak provozována majorita agendových informačních systémů zadavatele, které slouží k zajištění výkonu jeho veřejné správy a dále k zajištění interních činnosti a agend. Na této platformě jsou rovněž provozována adresářové služby a řízení uživatelských účtů a práv v nich. Z těchto důvodů je požadována kompatibilita s tímto technologickým prostředím a jako definice požadavku je uveden konkrétní produktový název.

# Záložní zdroj pro servery s příslušenstvím

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky.

| Parametr | Popis minimální úrovně parametru |
| --- | --- |
| Základní požadavky | Záložní zdroj napájení (UPS) |
| Pro montáž do 19" rozvaděče, výška základní jednotky max. 2U, při použití BP, max. celkově 4U |
| Maximální hloubka 75cm |
| Typ použitých baterií - bezúdržbové, hermeticky uzavřené, ventilem řízené olověné baterie |
| Výkonové požadavky | Při plném zatížení - zabezpečení provozu minimálně 15 minut |
| Parametry vstupního napětí - 220/230/240 V, 40 -70 Hz |
| Parametry výstupního napětí - 220/230/240 V (volitelné), 50 Hz/60 Hz (volitelné) |
| Max. nastavitelný výkon 2 700 W |
| Jmenovitý výkon 3 000 VA |
| Funkční požadavky | Topologie - On-line s dvojí konverzí |
| Přípojky:   * min. 8x IEC 320 C13 * min. 2x IEC 320 C19 |
| Přední ovládací panel s LCD, s akustickým a vizuálním varováním |
| Vzdálená správa a dohled pomocí síťové komunikace (požadavek na min. 10/100 Mbit síťový RJ45 konektor) |
| Podpora protokolů HTTPS, SSH, SNMPv2c a SNMPv3 |
| Požadavky na záruku a prodlouženou záruku | Záruka na UPS jako celek s výjimkou baterie min. 60 měsíců |
| Záruka na baterie min. 24 měsíců |

# Páteřní přepínač s příslušenstvím

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky.

| Parametr | Popis minimální úrovně parametru |
| --- | --- |
| Základní požadavky | Třída zařízení: L3 switch, podpora provozu jako ToR |
| Formát zařízení do racku |
| Velikost zařízení: max. 1U |
| min. 24x SFP/SFP+ 100M/1/10G portů s volitelným fyzickým rozhraním |
| min. 4x SFP/SFP+/SFP28/SFP56 1/10/25/50G portů s volitelným fyzickým rozhraním |
| Chlazení typu Front-to-Back |
| Všechny ethernet porty jsou dostupné zepředu |
| Výkonové požadavky | Celková propustnost přepínače min. 880 Gb/s |
| Celkový paketový výkon přepínače min. 650 Mpps |
| Propustnost stohovacího propojení min. 200 Gbps |
| Minimálně 8MB paketový buffer |
| 2x Hot-Swap zdroje min. 250W |
| Funkční požadavky | Podpora "jumbo rámců" včetně velikosti min. 9198 Byte |
| Podpora linkové agregace IEEE 802.3AX |
| Konfigurovatelné rozkládání LACP zátěže podle L2, L3 |
| Počet LACP skupin/linek ve skupině - min. 256/8 |
| Počet záznamů v tabulce MAC adres - min. 29 000 |
| Počet záznamů v tabulce ARP - min. 28 000 |
| Protokol pro definici šířených VLAN - MVRP |
| Podpora VLAN podle IEEE 802.1Q, minimálně 4 000 aktivních VLAN |
| VLAN translace - swap 802.1Q tagů na trunk portu |
| Podpora zařazování do VLAN podle standardu 802.1v |
| IEEE 802.1s - Multiple Spanning Tree |
| STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+) |
| Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED |
| Detekce jednosměrnosti optické linky (např. UDLD) |
| DHCP server |
| DHCP relay pro IPv4 a IPv6 |
| Podpora NTPv4 pro IPv4 a IPv6 včetně VRF a MD5 autentizace |
| Statické směrování IPv4 a IPv6 |
| Počet záznamů ve směrovací tabulce min. 64 000 |
| Dynamické směrování OSPFv2, OSPFv3 a BGP včetně podpory BFD |
| Podpora BGP a MP-BGP včetně podpory BFD |
| Podpora Layer-3 routed port |
| IGMP v2 a v3 |
| MLD v1 a v2 |
| Hardware podpora IPv4 a IPv6 ACL |
| ACL definice na základě skupiny fyzických portů |
| ACL aplikovatelný na interface, LAG, VLAN |
| BPDU a Root guard |
| DHCP snooping pro IPv4 a IPv6 |
| HW ochrana proti zahlcení portu (broadcast/multicast/icmp) nastavitelná na kbps a pps |
| 802.1x ověřování včetně více současných uživatelů na port, minimálně 32 uživatelů/port |
| Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou) |
| Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675 |
| Podpora Critical VLAN |
| Podpora uživatelských rolí definujících pro konkrétní uživatele více tagovaných či netagovaných VLAN, ACL, QoS politiky a SDN tunely. |
| Uživatelské role mohou být lokálně definované v přepínači nebo mohou být dynamicky stáhnuty z RADIUS serveru na základě výsledku autorizace. |
| Podpora IPv6 RA Guard |
| IP source guard / dynamic IP lockdown |
| Podpora Dynamic ARP protection |
| Port security |
| Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU |
| Podpora IPv4 a IPv6 QoS |
| IEEE 802.1p - minimální počet front - 8 |
| Management | CLI formou RJ45 serial konsole port |
| Konfigurace zařízení v člověku čitelné textové formě |
| OoB management formou portu RJ45 s podporou ethernetu |
| USB port pro přenos konfigurace a firmware |
| Podpora SSHv2, SFTP a HTTPS pro IPv4 a IPv6 |
| Podpora RSA s délkou klíče minimálně 4096 bitů |
| Podpora grafického uživatelského webového rozhraní. Možnost vytváření vlastních diagnostických a korelačních skriptů a jejich grafických interpretací v jazyce Python (korelace libovolných událostí a hodnot v podobě grafů) |
| Podpora SNMPv2c a SNMPv3 |
| Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL |
| TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting) |
| SPAN a ERSPAN port mirroring, alespoň 4 různé obousměrné session |
| TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logováni do více SYSLOG serverů |
| Podpora automatických i manuálních snapshotů systému a možnost automatického obnovení předchozí konfigurace v případě konfigurační chyby |
| Podpora standardního Linux Shellu (BASH) pro debugging a skriptování |
| Podpora skriptování v jazyce Python – lokální interpret jazyka v přepínači |
| Integrovaný nástroj na odchyt paketů (např. WireShark nebo ekvivalentní) |
| Interpretace uživatelských skriptů monitorujících definované parametry síťového provozu s možností automatické reakce na události |
| Interní SSD úložiště pro sběr provozních dat a pokročilou diagnostiku zařízení |
| Podpora OVSDB |
| Analýza síťového provozu sFlow podle RFC 3176 |
| Ochrana proti nahrání modifikovaného SW prostřednictvím image signing a secure boot, ověřující autentičnost a integritu OS prostřednictvím TPM chipu |
| Podpora integrace s automatizačními nástroji (Ansible, NAPALM) |
| Podpora REST API v režimech read-only a read-write pro automatizaci nastavení |
| Příslušenství - kabely a transceivery | Požadujeme dodání 1 ks SFP56 DAC kabel 0,65m, 10 ks SFP+ SM (10 km), 5 ks SFP+ MM (300m). |
| Záruka, záruční servis a technická podpora | Je požadována záruka na hardware s výměnou NBD v délce 60 měsíců. Tato záruka musí být garantovaná výrobcem zařízení. |
| Je požadován nárok na software aktualizace (nové verze programového vybavení) v minimální délce 60 měsíců. |
| Je požadovaná technická podpora výrobce po dobu min. 60 měsíců. |

# Backup server s příslušenstvím

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky.

| Parametr | Popis minimální úrovně parametru |
| --- | --- |
| Základní a výkonové požadavky | **Typ zařízení -** Šasi pro montáž do standardního racku o velikosti max. 2U. Požadujeme dodání serveru s rackmount příslušenstvím včetně pohyblivého ramene pro zachycení kabeláže |
| **Procesor -** CPU - architektura x86 s 16 plnohodnotnými jádry. V testu na cpubenchmark.net minimálně 40 000 bodů. Max. počet CPU je omezen na 1 a počet jader je omezen na 16 core z důvodu licencování OS a aplikací. |
| **Paměť**   * 128GB, min. typu DDR4 s taktem 3200MT/s, Dual Rank |
| **Řadič datového diskového systému - minimální požadované vlastnosti**   * typu SAS, min. x8 PCI Express 3.1 kompatibilní, dvoukanálový (2 konektory) * podpora RAID 0, 1, 5, 6, 10, 50, 60 * podpora 6/12Gbps technologie rozhraní disků, 12Gbps na port * podpora Online Capacity Expansion (OCE) * podpora Online RAID Level Migration (RLM) * podpora Auto resume po ztrátě napájení * podpora disků s formátem bloku 512n/512e/4Kn * podpora TRIM/UNMAP příkazů pro SAS/SATA SSDs * podpora šifrování dat na discích (SED) * přímý přístup na SSD * podpora S.M.A.R.T. * podpora globálního i dedikovaného hot-spare * min. 4GB cache, zálohované akumulátorem |
| **Pevné disky**   * Server musí být osaditelný min. 14x disky SATA, SAS HDD a SSD. Veškeré potřebné komponenty (řadič, diskové pozice, kabeláž, napájecí zdroje apod.) musí být součástí dodávky tak, aby server bylo možné funkčně osadit plným počtem HDD pouhým dodatečným vložením disků. * Požadujeme dodání 2 ks disků min. 3.84TB SATA/SAS SSD, DWPD 1, hot-swap a 8 ks disků min. 8TB, SATA/SAS, 7.2K 512e hot-swap |
| **LAN konektivita**   * min. 1ks Ethernet adapter Dual Port 10/25GbE Adapter včetně 2 ks SFP+ MM zářičů a 2m kabelů LC/LC-LC/LC.. Karta bude od stejného výrobce jako u produkčních serverů, které jsou součástí tohoto plnění, je požadována plná kompatibilita. * min. 1ks Ethernet adapter 2x 1GbE 1000BASE-T * min. 1ks 8Gb Single Port Fibre Channel Host Bus Adapter, kompatibilita s poptávanou páskovou knihovnou |
| **Napájení a chlazení**   * Server musí být vybaven redundantním napájením a chlazením, hot-plug vyměnitelné za provozu * 2ks hot-swap zdroje napájení dimenzované pro plné osazení serveru disky, CPU, RAM a PCIe zařízení, účinnost min. 96% |
| Funkční požadavky | Server musí být osazen TPM 2.0 |
| Vyčítání přes SNMP celkového zdraví serveru bez nutnosti instalovat OS – jeden parametr v MIB |
| IPMI 2.0 popř. obdoba, možnost vzdáleného převzetí grafické konsole bez závislosti na OS, webový klient HTML5, vzdálený mount DVD media, USB, dedikovaný port (není součástí požadovaného počtu ethernet portů) |
| Záruka, záruční servis a technická podpora | Je požadována záruka na dobu 5 let s reakční dobou na založený incident na kompletní HW a přístup k technické podpoře 24x7, 4h |
| Servisní zásahy provádí technik s příslušnou znalostí, schválený výrobcem |
| Nárok na aktualizace systému dostupné min. po dobu záruky, nabízené přehledně v servisním portálu po zadání sériového čísla |

# Bezpečné datové úložiště

*(v projektovém záměru zadavatele uvedené jako Veeam hardened repository, dodavatel není vázán konkrétním produktovým označením pro podání nabídky)*

Každý kus zařízení musí splňovat následující minimální technické požadavky.

| Parametr | Popis minimální úrovně parametru |
| --- | --- |
| Základní a výkonové požadavky | **Typ zařízení**   * Šasi pro montáž do standardního racku o velikosti max. 2U. Požadujeme dodání serveru s rackmount příslušenstvím včetně pohyblivého ramene pro zachycení kabeláže |
| **Procesor** CPU - architektura x86 s 16 plnohodnotnými jádry. V testu na cpubenchmark.net minimálně 40 000 bodů. Max. počet CPU je omezen na 1 a počet jader je omezen na 16 core z důvodu licencování OS a aplikací. |
| **Paměť**   * 32GB, min. typu DDR4 s taktem 3200MT/s, Dual Rank * Možnost zvýšení kapacity na dvojnásobek, 64GB při použití identických modulů, bez nutnosti výměny dodaných |
| **Řadič datového diskového systému - minimální požadované vlastnosti**   * typu SAS, min. x8 PCI Express 3.1 kompatibilní, dvoukanálový (2 konektory) * podpora RAID 0, 1, 5, 6, 10, 50, 60 * podpora 6/12Gbps technologie rozhraní disků, 12Gbps na port * podpora Auto resume po ztrátě napájení * podpora disků s formátem bloku 512n/512e/4Kn * podpora šifrování dat na discích (SED) * přímý přístup na SSD * podpora S.M.A.R.T. * podpora globálního i dedikovaného hot-spare * minimálně 4GB cache, zálohované akumulátorem |
| **Pevné disky**   * Server musí být osaditelný min. 12x disky SATA, SAS HDD a SSD. Veškeré potřebné komponenty (řadič, diskové pozice, kabeláž, napájecí zdroje apod.) musí být již součástí dodávky tak, aby server bylo možné funkčně osadit plným počtem HDD pouhým dodatečným vložením disků. * Požadujeme dodat 12 ks disků 3,5" min. 8TB, SATA/SAS, min. 7.2K 512e hot-swap |
| **LAN konektivita**   * min. 1ks Ethernet adapter Dual Port 10/25GbE Adapter včetně 2 ks SFP+ MM zářičů a 2m kabelů LC/LC-LC/LC. * min. 1ks Ethernet adapter 2x 1GbE 1000BASE-T |
| **Napájení a chlazení**   * Server musí být vybaven redundantním napájením a chlazením, hot-plug vyměnitelné za provozu * 2ks hot-swap zdroje - napájení dimenzované pro plné osazení serveru disky, CPU, RAM a PCIe zařízení, účinnost min. 96% |
| Kompatibilita | Plná kompatibilita se stávající platformou zálohování zadavatele Veeam |
| Funkční požadavky | Server musí být osazen TPM 2.0 |
| Vyčítání přes SNMP celkového zdraví serveru bez nutnosti instalovat OS – jeden parametr v MIB |
| IPMI 2.0 popř. obdoba, možnost vzdáleného převzetí grafické konsole bez závislosti na OS, webový klient HTML5, vzdálený mount DVD media, USB, dedikovaný port (není součástí požadovaného počtu ethernet portů) |
| Záruka, záruční servis a technická podpora | Je požadována záruka na dobu 5 let s reakční dobou na založený incident do konce následujícího pracovního dne (NBD) |
| Servisní zásahy provádí technik s příslušnou znalostí, schválený výrobcem |
| Nárok na aktualizace systému dostupné min. po dobu záruky, nabízené přehledně v servisním portálu po zadání sériového čísla |

# Pásková knihovna

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky.

| Parametr | Popis minimální úrovně parametru |
| --- | --- |
| Základní a výkonové požadavky | **Typ zařízení -** Pásková knihovna pro montáž do standardního racku o velikosti max. 2U, včetně ližin pro její uchycení |
| **Typ a počet mechanik -** 1× LTO-9 mechanika s FC připojením |
| **Počet slotů na pásky -** min. 24 slotů na pásky |
| **Pásky**   * 20× páska LTO-9 - požadovaná nativní kapacita min. 18TB * 1× čisticí páska * Pásky musí být již z výroby označeny příslušnými čárovými kódy, případně musí být dodán potřebný počet samolepících etiket s páskám odpovídajícími čárovými kódy |
| Management | LCD s ovládáním pro místní správu |
| 1x RJ-45 port 10/100Mbps pro vzdálenou správu |
| Kompatibilita se zálohovacím SW Veeam Backup&Replication - jedná se o stávající platformu zálohování provozovanou zadavatelem |
| Záruka, záruční servis a technická podpora | Je požadována záruka 5 let s podporou dostupnou 24×7 s reakční dobou následující pracovní den (NBD) od nahlášení závady, a to v místě instalace (on-site) |
| Podpora musí zahrnovat možnost přístupu k dokumentaci a aktualizacím software minimálně po dobu záruky a to včetně nároku na jejich stažení a užití. |

# Požadavky na instalační a implementační práce

Dodané řešení bude sloužit pro jako vysoce dostupná hyperkonvergovaná infrastruktura pro chod agendových IS úřadu a jeho zálohování. Dodávka musí obsahovat kompletní instalaci a implementaci řešení, nad kterým pak bude v režii kupujícího se třetí stranou provedena implementace agendových systémů (virtuální databázové, aplikační a komunikační servery) a konfigurace úloh pro zálohování nově vytvořených virtuálních serverů s agendovými IS.

Implementace dodávaného řešení bude provedena po odsouhlasení zadavatelem a v souladu s „best practice“ a dle doporučení výrobců jednotlivých komponent dodávaného řešení k datu realizace plnění.

Náklady na provedení implementačních služeb musí být zahrnuty v nabídkové ceně k položce, ke které se vztahují a nelze je vyčíslit zvlášť.

Základní popis prostředí kupujícího:

* Existují dvě oddělená datová centra, DC1 a DC2.
* V DC1 jsou umístěny 2 virtualizační hosti (VMware platforma), společně s diskovým úložištěm. V DC2 je umístěn backup server s úložištěm záloh a páskovou knihovnou.
* Optické SM kabely mezi datovými centry DC1 a DC2 je zakončen v optických vanách LC konektory.
* Jako router a firewall aktuálně slouží dvojice appliancí Fortinet Fortigate FG-100D v režimu HA. Jsou umístěny v datovém centru DC1.
* Konektivita do Internetu je zakončena v datovém centru DC1.
* Stávající síťové prvky jsou monitorovány pomocí SNMP nástrojem PRTG.

## Specifikace konkrétních instalačních a implementačních požadavků

Dodaná zařízení budou umístěna především do dvou oddělených datových center DC1 a DC2. Přístupové přepínače, záložní zdroje pro tyto přepínače a přístupové body (AP) budou rozmístěny po dalších prostorech města, které budou upřesněny v rámci zpracování implementační dokumentace ze strany kupujícího.

V rámci přípravných prací:

* návrh migrace na nové firewally, předložení převodní tabulky FW pravidel a dalších nastavení
* návrh segmentace sítě pro nově nasazované technologie (minimálně oddělení jednotlivých typů komunikace do samostatných VLAN)
* návrh adresního plánu pro potřeby nově nasazovaných technologií s ohledem na segmentaci stávající sítě v budoucnu
* návrh konvence DNS názvů pro jednotlivá zařízení
* návrh a nasazení oddělené sítě pro správu

V rámci instalačních a implementačních prací:

* dodávka požadovaného hardware a software
* doprava hardware do místa instalace
* montáž dodaných zařízení do stávajících datových rozvaděčů
* redundantní zapojení napájení jednotlivých zařízení mimo a přes pro ně vyhrazené UPS
* konfigurace portů pro správu a karet pro vzdálenou správu jednotlivých zařízení a jejich připojení do vyhrazené sítě pro správu
* aktualizace firmware v jednotlivých zařízeních a jejich komponentách na nejnovější doporučené verze
* zabezpečení přístupu ke správě jednotlivých zařízení, konfigurace synchronizace jejich času, konfigurace SNMP parametrů pro možnost vzdáleného dohledu, konfigurace SMTP pro zasílání e-mailové notifikace o stavu zařízení
* sestohování páteřních přepínačů a přístupových přepínačů a jejich propojení
* zprovoznění managementu síťového prostředí, včetně zavedení 802.1x
* konfigurace agregačních skupin (LACP) na přepínačích pro propojení přepínačů, připojení serverů
* konfigurace VLAN, trunk portů a přístupových portů na jednotlivých přepínačích
* nasazení Spanning-Tree protokolu (MSTP) na síťových prvcích
* instalace a konfigurace hypervizoru VMware ESXi na příslušných serverech
* instalace a konfigurace serveru VMware vCenter Appliance pro správu virtualizační infrastruktury
* nasazení a konfigurace distribuovaných switchů (vDS), vMotion komunikace, HA clusteru
* instalace a konfigurace softwarově definovaného úložiště VMware vSAN (2-node vSAN Stretched Cluster s vSAN Witness Appliance)
* instalace operačního systému a jeho aktualizací na zálohovací server, instalace ovladačů a nástrojů pro správu od výrobce serveru
* instalace zálohovacího software Veeam na zálohovací server a jeho konfigurace (bez konfigurace zálohovacích úloh)
* připojení páskové knihovny a bezpečného datového úložiště k zálohovacímu serveru
* Instalace a konfigurace nástroje pro logování infrastruktury, připojení monitorovaných zařízení včetně distribuce Windows agenta na pracovní stanice a servery. Vytvoření přehledového dashboardu a výstupů pro obsluhu
* nastavení pravidelných self-testů UPS a e-mailové notifikace o výsledku těchto testů
* konfigurace UPS a instalace software na servery a jejich konfigurace pro řízené vypínání serverů v případě výpadku napájení
* aplikace licencí
* kompletní ověření funkčnosti celého řešení
  + vytvoření testovacích virtuálních serverů ve virtualizační infrastruktuře
  + simulovaný výpadek jednoho z páteřních přepínačů
  + odpojení jednoho z propojů mezi páteřními přepínači
  + otestování odstávky jednoho z nodů VMware vSAN clusteru (plánovaná i neplánovaná)
  + otestování funkcionality VMware HA a restartu testovacího virtuálního serveru v druhé lokalitě
  + simulovaný výpadek celé jedné lokality (datového centra)
  + otestování redundantního napájení jednotlivých zařízení střídavým odpojením jednoho z napájecích zdrojů
  + otestování funkčnosti korektního vypnutí jednotlivých serverů při výpadku napájení
  + otestování funkčnosti vypnutí celé infrastruktury při výpadku napájení a jejího korektního nastartování po obnovení napájení
* propojení celého řešení do stávající síťové infrastruktury
* zpracování podrobné dokumentace skutečného provedení
* provedení akceptačních testů

## Obecné požadavky

Kupující v rámci plnění požaduje provést implementační práce na dodaných HW a SW komponentách. Konkrétní požadované práce v závislosti na předmětu dodávky jsou specifikovány výše. Dodavatel je povinen zahrnout do nabídky i veškeré další činnosti a prostředky, které jsou nezbytné pro řádné provedení plnění v rozsahu doporučeném výrobci a dle tzv. nejlepších praktik, i v případě, pokud nejsou explicitně uvedeny, ale jsou pro realizaci předmětu plnění podstatné.

Implementační služby budou minimálně v následujícím rozsahu:

* zpracování předimplementační analýzy
* zpracování prováděcí dokumentace
* zajištění projektového vedení realizace předmětu plnění
* dodávku nabízeného hardware a software
* kompletní implementaci řešení splňující povinné a nabízené parametry technického řešení
* zpracování dokumentace skutečného provedení
* zaškolení administrátorů
* zajištění zkušebního provozu
* provedení akceptačních testů
* předání do ostrého provozu
* zajištění ostatních služeb potřebných pro realizaci projektu

Veškerá dokumentace musí být zhotovena výhradně v českém jazyce, bude dodána v elektronické formě ve standartních formátech (např. MS Office) používaných zadavatelem na datovém nosiči a 1x kopii v papírové formě.

## Požadavky na předimplementační analýzu

Dodavatel před implementací řešení zpracuje předimplementační analýzu, minimálně pro následující oblasti:

* způsob začlenění nabízeného řešení do stávajícího ICT prostředí
* analýza požadavků na síťovou infrastrukturu
* analýza požadavků na ukládání a zálohování dat, obnovu dat, toky a objemy dat
* požadavky na rekonfigurace stávajících systémů ve vztahu k plánovanému využití
* dopady implementace na dostupnost a funkčnost stávajících služeb
* další podklady relevantní pro návrh řešení
* požadovaná součinnost kupujícího
* návrh opatření k odstranění neshod zjištěných v průběhu analýzy.

Výstupem předimplementační analýzy bude písemná zpráva podléhající schválení kupujícím.

## Požadavky na zpracování prováděcí dokumentace

Dodavatel před zahájením implementačních prací zpracuje prováděcí dokumentaci, která bude důsledně vycházet z předimplementační analýzy a bude zahrnovat všechny aktivity potřebné pro řádné zajištění implementace předmětu plnění.

Prováděcí dokumentace musí být před zahájením prací písemně schválena Kupujícím.

Prováděcí dokumentace musí zohlednit podmínky stávajícího stavu, požadavky cílového stavu a musí obsahovat minimálně tyto části:

* detailní popis cílového stavu včetně popisu funkcionalit jednotlivých HW a SW částí systému
* způsob zajištění koordinace realizace předmětu plnění s běžným provozem
* detailní návrh a popis postupu implementace předmětu plnění
* detailní popis zajištění bezpečnosti informací
* detailní harmonogram projektu včetně uvedení kritických milníků
* návrh designu úložišť a virtuálních serverů a jeho konfigurace
* návrh designu zálohování a jeho konfigurace
* návrh designu síťového řešení a jeho konfigurace
* návrh monitorování řešení monitorovacími nástroji
* vazby na stávající systémy a jejich konfigurace
* návrh akceptačních kritérií a akceptačních testů
* detailní popis navrhovaných školení

## Požadavky na zajištění projektového řízení

Dodavatel zajistí projektové řízení po celou dobu realizace plnění certifikovaným specialistou. Součástí nabídky Dodavatele bude popis metodiky, která bude použita pro projektové řízení.

## Požadavky na zaškolení

Dodavatel zajistí zaškolení zaměstnanců Zadavatele – administrátorů – na zařízení a systémy, v rámci tohoto plnění, a to minimálně v rozsahu předávané provozní dokumentace.

* zaškolení zajistí seznámení specialistů IT kupujícího se všemi podstatnými částmi plnění v rozsahu potřebném pro provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin.
* Minimální rozsah zaškolení je 8 hodin.
* Zaškolení bude probíhat v sídle kupujícího.
* Předpokládá se účast 2 administrátorů.

## Požadavky na provedení zkušebního provozu a akceptačních testů

* Dodavatel zajistí pro realizovanou část zkušební provoz v délce minimálně 10 dnů se zajištěním technické podpory specialistů na dodané řešení s možností nahlášení požadavku v pracovní den v době od 8 hod. do 16 hod. a dobou reakce od nahlášení požadavku do 4 hod.
* Dodavatel navrhne způsob a provedení akceptačních testů, který bude podléhat schválení ze strany kupujícího
* Součástí akceptačních testů musí být minimálně kompletní ověření funkčnosti celého řešení dle této specifikace
* O provedení akceptace a jejím výsledku musí být vyhotoven písemný protokol.
* Přechodem do ostrého provozu se rozumí okamžik úspěšné akceptace plnění včetně vypořádání všech vad a nedodělků.

## Další požadavky na záruky, záruční servis a další podmínky v rámci záruky

* Nabídne-li Dodavatel v rámci svého řešení HW, na něž výrobce standardně (tj. v rámci standardní dodávky a ceny) poskytuje horší záruku, popř. podporu, požaduje Zadavatel zahrnout do nabídky cenu povýšení záruky, popř. podpory na jím požadovanou úroveň.
* kupující požaduje přístup k aktualizacím software a firmware dodaného HW v kupní ceně minimálně po dobu záruky.
* Veškeré opravy po dobu záruky budou provedeny bez dalších nákladů pro kupujícího
* Není-li uvedeno u dané položky požadovaného HW jinak, požaduje zadavatel provedení záruční opravy do deseti pracovních dnů.
* Pro hlášení požadavků na záruční opravy zajistí prodávající kupujícímu přístup ke svému helpdeskovému systém s on-line přístupem pro nahlášení a správu požadavků včetně uchování historie požadavků a jejich řešení. Popis helpdeskového systému musí být součástí nabídky. Provozní doba helpdeskového systému musí být minimálně 7-16 hod. v pracovních dnech.

# Harmonogram plnění

Kupující požaduje dodržení následujícího harmonogramu plnění – zde jsou uvedeny maximální možné lhůty pro realizaci dodávky. Údaj D značí datum nabytí účinnosti kupní smlouvy. Čísla značí počet kalendářních dnů.

| Aktivita | Začátek | Termín splnění |
| --- | --- | --- |
| Nabytí účinnosti smlouvy (uveřejnění v registru smluv) | D | D |
| Zahájení projektu – úvodní projektová schůzka | D | D+7 |
| Předimplementační analýza - zpracování | D+7 | D+17 |
| Předimplementační analýza – připomínkové řízení, schválení | D+17 | D+24 |
| Prováděcí dokumentace – zpracování | D+24 | D+34 |
| Prováděcí dokumentace – připomínkové řízení, schválení | D+34 | D+40 |
| Realizace předmětu plnění | D+40 | D+80 |
| Školení administrátorů | D+80 | D+90 |
| Zkušební provoz | D+90 | D+110 |
| Akceptační testy | D+110 | D+120 |
| Zahájení ostrého provozu | D+120 | - |

Dodavatel může dle svého uvážení výše uvedené maximální lhůty trvání zkrátit při dodržení všech částí předmětu plnění a bez snížení kvality dodávaných služeb.

Maximální lhůty trvání nesmí Dodavatel při tvorbě detailního harmonogramu prodloužit.

Detailní harmonogram plnění uvede Dodavatel ve své nabídce.

Dodavatel uvede potřebnou součinnost kupujícího pro splnění harmonogramu plnění ve své nabídce.

# Návaznost na projektový záměr kupujícího

**Realizací tohoto projektového záměru kupující sleduje následující cíl projektu IROP, který musí být realizací plnění dosažen a tedy prodávajícím zohledněn do jeho nabídkové ceny a realizovaného plnění jako jeho součást:**

*V rámci realizace projektu dojde k nasazení redundance serverů a současně vytvoření geograficky odděleného clusteru serverových prostředků určených pro provoz informačních systémů. Ze stávajícího prostředí v lokalitě A dojde k přesunutí druhého ze stávající virtualizačních serverů do lokality B a současně k rozšíření obou lokalit o nový server do každé. Takovým způsobem dojde k vybudování nového řešení s odpovídajícím rozmístěním systémových prostředků. Takové rozmístění bude takovým způsobem rovnoměrné a stejné. Díky tomu bude možné v obou prostředích aplikovat stejná pravidla a stejné užití nově rozšířených serverových systémových prostředků, než kdyby došlo ke komplexně novému vybavení druhé lokality, která by byla nepoměrná vůči stávajícímu vybavení a vytvářela by další specifické překážky pro dosažení plnohodnotné redundance mezi jednotlivými technologickými místnostmi. Nasazené nové servery vedle serverů stávajících budou dimenzovány (konkrétní požadavky na dimenzaci jsou uvedeny výše v této technické specifikaci) tak, aby dokázaly pokrýt zvýšené nároky na dostupnost informačních systémů, včetně jejich rozvoje, když došlo s růstem datových sad za dobu jejich provozu a rozvojem elektronizace i k nárůstům požadavků informačních systémů na serverové systémové prostředky za účelem zajištění zvýšené dostupnosti takových prostředků pro zabezpečované informační systémy.*

Další služby potřebné s přesunem technologií a souvislosti s dodávkou předmětu plnění za účelem vzniku výše uvedené serverové redundance jsou prodávajícím zohledněny v jeho ceně plnění. Dvě konkrétní serverové místnosti jsou uvedeny v kupní smlouvě.