

Specifické parametry nabízeného řešení

K1 - Virtualizační platforma a K2 – Zabezpečení LAN a Wifi

Virtualizační server 1x

- Nabízený server **HPE DL360 Gen11 8SFF CTO Server** je v rackovém provedení 2U včetně výsuvných kolejnic a montážního materiálu do racku
- CPU Intel Xeon Silver 4410Y - 1x procesor 16 jádrový s výkonem 23971 bodů v testu CPU mark (dle webu <https://www.passmark.com/>) v době podání nabídky
- RAM: 128 GB, 3200 MT/s
- Rozšiřitelnost: 256 GB bez výměny modulů
- SSD: 3x 3,84TB, SSD
- SSD: 2x 240GB, SSD
- RAID: SAS12Gb, RAID 5, zálohovaná write back cache 4GB
- LAN: LAN 2x10Gb SFP+ s podporou virtualizace - VMware NetQueue, Microsoft VMQ. Podpora NIC partitioning (NPAR) a iSCSI offload
- Management: Servisní modul s možností samostatného přístupu po management síti, možnost vzdálené klávesnice, myši a obrazovky bez nutnosti běhu OS, možnost zapínat a vypínat server, možnost bootování se vzdáleného média. Vyhrazený LAN port, podpora http/s, ssh, SNMP, syslog. Okamžité a historické hodnoty teplot a napájení. Podpora vícefaktorového ověřování (autentizace)
- Provozní podmínky: určen pro provoz v běžném neklimatizovaném prostředí do 40 (nárazově až 45) stupňů Celsia
- Napájení: 2x napájecí zdroj, redundance, 750W, Platinum specifikace dle 80 PLUS https://cs.wikipedia.org/wiki/80_Plus
- Management: Stavové informace na čelním panelu s výraznou indikací nestandardních a chybových provozních stavů či parametrů (min. napájení, teplota, vada HDD. Aktivní indikace standardního provozního stavu.
- Záruka 60 měsíců zajištěná výrobcem, v místě instalace v režimu NBD

SW licence operačních systémů

- 2 ks licencí **Microsoft® Win Server Standard Core 2022 SLng 16L** - 64-bitového serverového operačního systému v aktuální verzi. Každá licence umožňuje provoz 2 virtuálních serverů stejné verze v prostředí nabízené serverové virtualizace, dále provoz všech nabízených aplikací a management nástrojů.
- 50 ks licencí Win Server CAL 2022 SLng DCAL

SW licence virtualizace

- 1 ks licence **Microsoft® Win Server Standard Core 2022 SLng 16L** - Software pro virtualizaci serverů včetně management konzole
- Funkcionalita, která bude provádět diskovou zálohu a jednoduchou obnovu na úrovni image virtuálních strojů nebo jednotlivých souborů
- Komplexní správa virtuální infrastruktury z jedné konzole a umožňující integraci s produkty třetích stran
- Podpora operačních systémů Windows 2000 a novější, Linux, FreeBSD jako OS ve virtuálních strojích

UPS 1x

- UPS **Eaton 5PX 2200i RT2U Netpack, UPS 2200VA**, 8 zásuvek IEC, LCD v provedení do racku, max. 2U, včetně montážního materiálu
- Elektrické provedení - jmenovité napětí 230 V, jednofázová na vstupu i výstupu
- Výkon - 2200 VA / 1980 W
- Technologie - Síťově interaktivní
- Účinnost: 97%, výstupní účinník 0,9
- Stabilizace: Výstupní napětí – 230 V max. +6%/-10%
- Kapacita: Doba běhu na baterie 5 min při 50% zátěži

- Vstup: Zásuvka IEC C14 (16 A)
- Výstupy: 8 zásuvek IEC C13, 2 zásuvka IEC C19
- Napájecí segmenty: 2 nezávisle ovládané napájecí segmenty pro postupný náběh napájených technologií
- Diagnostika: Vestavěný úplný systémový autotest, možnost automatického plánovaného provádění
- Servis: Baterie vyměnitelné za chodu, aniž by bylo nutné odstavovat připojená zařízení.
- Komunikační porty: RS-232, USB, vzdálené zapnutí/vypnutí, LAN management port
- Stavové informace: Stavový grafický displej pro konfiguraci a základní informace o stavu UPS
- Řízení: Schopnost ovládání a restartování nabízeného serveru, korektní shutdown operačních systémů
- SW kompatibilita: UPS plně podporovaná výrobcem pro použití ve virtualizačních prostředích VMware a Microsoft Hyper-V, příslušný SW bude součástí dodávky
- Záruka 24 měsíců

SW licence zálohovací software

- Licence zálohovacího software **Veeam Backup Essentials Enterprise** EDU pro nabízený server bez omezení počtu zálohovaných virtuálních serverů a objemu dat.
- Efektivita ukládání dat - Integrované technologie komprimace a deduplikace.
- Nároky na správu - „Bezagentové“ řešení – bez instalace agentů do zálohovaných virtuálních serverů či aplikací
- Ochrana dat- provádění datově konzistentních záloh hlavních serverových aplikací – Microsoft SQL server, Active Directory, souborové systémy – bez nutnosti odstávky aplikace
- Fyzický server - vestavěná podpora zálohování stávajících fyzických serverů - pro fyzické servery je přípustné využívat agenty
- Podpora WAN - možnost plnohodnotné replikace přes WAN pro replikaci virtuálních serverů do vzdálených lokalit (např. Technologického centra Plzeňského kraje)
- Snapshoty - využívání snapshotů, zálohování pouze dat změněných od poslední úspěšné zálohy
- Kompatibilita - podpora operačních systémů Windows a Linux v zálohovaných virtuálních serverech
- Úložiště záloh - možnost ukládání záloh na diskový prostor a páskovou jednotku/knihovnu
- Podpora DR - možnost nouzového spuštění zazálohovaného virtuálního serveru z NAS v izolovaném prostředí bez nutnosti obnovy
- Správa - běžné úlohy obnovy (obnovení souboru, databáze SQL, objekty Active Directory) provádět pomocí průvodců.
- Správa - automatický reporting úspěšných i neúspěšných úloh, běžné úlohy obnovy (obnovení souboru, databáze SQL, objekty Active Directory) lze provádět pomocí průvodců.
- Vlastnosti produktu
https://www.veeam.com/cz/veeam_availability_suite_9_5_editions_comparison_ds.pdf
- Záruka 60 měsíců včetně nároku na opravné verze (požadováno 12 měsíců)

Síťové úložiště NAS 1x

- Síťové úložiště **NAS Synology RS822RP+** k umístění do RACKu.
- Výkon 64 bit CPU, 4 jádra
- 4 pozice pro HDD, rozšiřitelné min na 8 HDD s rozšiřující jednotkou
- Rozšiřitelnost - podpora připojení externích disků přes USB 3.0 (4 porty)
- Hot-swap - disky vyměnitelné za chodu.
- SSD HDD podpora SSD disků pro ukládání dat i akceleraci rotačních HDD
- HDD Osazeno 4x 8TB HDD SATAIII/64MB cache určených výrobcem pro NAS (nepřipouští se HDD určené jiným účelům (desktop, kamerové systémy apod.).
- Konektivita - 4 x 1Gbit Ethernet porty s podporou agregace linek a redundance, 2x 10Gbit SFP+.
- Výkon - Sekvenční výkon 1 500 MB/s čtení a 560 MB/s zápis.
- Kompatibilita - plná podpora Microsoft Hyper-V a Windows ADS a ACL.
- Komunikace LAN - síťové protokoly CIFS, WebDAV, iSCSI, SSH, SNMP, http/s
- UPS - podpora korektního vypnutí signálem z UPS přes LAN při výpadku napájení
- Ochrana dat - Integrované typy ochrany dat RAID 1, RAID 5, RAID 6, RAID 10
- Záruka 36 měsíců včetně HDD

Firewall 1x

- Firewall **FortiGate 60F**, HW + 24x7 Unified (UTM) Protection 5YR
- Porty 9x 1GbE, dedikovaný port RJ45 pro DMZ, Konzolový port pro management a USB 3.0 port pro zálohu konfigurace
- Propustnost 9 Gbps pro velikost paketu 512byte
- Počet souběžných spojení 0,64 miliónu
- Propustnost SSL-VPN 900 Mbps, při licenčním nebo technickém omezení počtu klientů 50 klientů
- Propustnost IPS – 1,4 Gbps
- Propustnost SSL inspekce - 630 Mbps
- Kombinovaná propustnost: Firewall – aktivní IPS + aplikační kontrola + antimalware min. 1 Gbps pro běžný provoz
- Virtualizace - 10 virtuálních kontextů (požadováno 10)
- Vysoká dostupnost - režimy Active/Passive i Active/Active se společnou konfigurací
- Dualstack - podpora současného běhu IPv4 a IPv6
- Aplikační kontrola - detekce, monitoring, povolení či zakázání obvyklých síťových aplikací na základě signatury dané aplikace, nikoliv dle portu. Kontrola komunikace v SSL šifrovaných protokolech (HTTPS, IMAPS, POP3S)
- Antivir - antivirus pro vybrané protokoly, možnost volby různých databází, podpora archivace škodlivého obsahu, podpora protokolu ICAP pro offload AV engine, možnost detekce tzv. Grayware (rootkit, malware, spyware, keylogger, atd)
- Kategorizace a blokáce provozu je 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
- Antispam - antispamová a antivirová inspekce elektronické pošty
- Bezpečnost - automatická aktualizace UTM funkcí poskytovaná výrobcem zařízení
- Ověřování - LDAP, Active Directory, Single Sign On vůči Active Directory, Radius, TACACS+, Ověřování na základě certifikátu
- Management a monitoring přes HTTP/S, SSH, SNMP, syslog,
- Sledování toků - export síťových toků Netflow
- Standardní funkce - NAT, statické a dynamické routování, publikace interních serverů
- Záruka 60 měsíců v režimu 24x7. Odeslání náhradního zařízení max. následující den po nahlášení závady, včetně nároku na bezpečnostní aktualizace firmware a UTM (URL filtrace, IPS, antimalware, antispam, aplikační kontrola). Vadné zařízení se vrací výrobce až po obdržení náhradního.

Páteřní přepínač 1x

- Páteřní přepínač **Aruba 6300M 24SFP+ 4SFP56**
- Základní parametry: L3 switch v provedení 19"
- Propustnost: neblokovaná architektura
- Napájení: Redundantní hot-swap zdroje
- Chlazení: Vyměnitelné, hot-swap ventilátory
- Porty: 24x 1/10Gbps SFP+
- Uplink porty: 2x SFP56 s podporou 10/25/50Gbps
- Celkový paketový výkon přepínače: 650 Mpps
- Celková propustnost přepínače: 870 Gbit/s
- Stohování: Podpora 4 přepínačů ve stohu
- Agregace portů: podpora linkové agregace IEEE 802.1AX
- Dualstack: IPv4 a IPv6 dualstack včetně podpory ACL a QoS
- VLAN: VLAN 802.1Q, MAC i protocol based, podpora zařazování do VLAN a přidělení QoS a přístupových filtrů na základě 802.1X ověření
- Ověřování uživatelů a zařízení: podpora 802.1X
- Monitoring a správa: plná podpora CLI, SSH, SNMP 1-3, syslog, sFlow, RMON, web rozhraní
- Záruka: 60 měsíců v režimu NBD, odeslání náhradního zařízení max. následující pracovní den po nahlášení závady, včetně nároku na aktuální verze firmware

Přístupové přepínače 4x

- Základní parametry: Základní L3 přepínač v rackovém provedení max. 1U
- Stohování: podpora stohování pro jednotný management (přepínače musí stohovatelně vzájemně bez ohledu na provedení - viz. Porty a propustnost), 8 ks ve stohu
- Propustnost: neblokovaná architektura
- Celkový paketový výkon přepínače: Minimálně 130 Mpp
- Agregace portů: podpora LACP
- Dualstack: IPv4 a IPv6 dualstack včetně podpory ACL a QoS.
- VLAN: VLAN 802.1Q, MAC i protocol based, podpora zařazování do VLAN a přidělení QoS a přístupových filtrů na základě 802.1X ověření
- Ověřování uživatelů a zařízení: podpora 802.1X
- Monitoring a správa: plná podpora CLI, SSH, SNMP 1-3, syslog, sFlow, RMON, web rozhraní
- Záruka: 60 měsíců v režimu NBD, odeslání náhradního zařízení max. následující pracovní den po nahlášení závady, včetně nároku na aktuální verze firmware

Nabízené modely:

- 2 kusy - **Aruba 6100 48G CL4 PoE 4SFP+ 370W Switch**
- 1 kus - **Aruba 6100 12G CL4 PoE 2G/2SFP+ 139W Switch**
- 1 kus - **Aruba 6100 24G CL4 PoE 4SFP+ 370W Switch**
- Součástí dodávky switchů jsou potřebné propojovací LAN kabely a SFP moduly

WiFi přístupové body (AP) 10x

- Přístupový bod (AP) WiFi **Aruba AP-505 (RW) Unified AP**
- Držák pro montáž na stěnu nebo strop
- Ap pracuje v radiovém pásmu 2,4 a 5 GHz současně, 2 radiové moduly
- interní systém min. MIMO 2,4GHz rádio: 2x2:2 a 5GHz rádio: 2x2:2, optimalizovaný pro montáž na strop
- Minimální komunikační rychlost na fyzické vrstvě (Max data rate) pro 5GHz min. 1200 Mbps a pro 2.4GHz min.: 570 Mbps
- Plnohodnotná certifikace Wi-Fi Alliance, min. IEEE 802.11a/b/g/n/ac, a 802.1x včetně přiřazování do VLAN
- automatické směrování komunikace klientů z 2.4 GHz na 5 GHz (pokud klienti podporují obě pásma)
- průběžná detekce non-WiFi rušení a spektrální analýza
- podpora vysílání min. 16 SSID (WiFi sítí) současně, podpora přiřazení každého SSID samostatné VLAN
- 1x 1Gb, PoE s podporou standardů 802.3at a 802.3af
- podpora standardu 802.3az - Energy-Efficient Ethernet (EEE)
- klasifikace a kontrola provozu, detekce obvyklých aplikací s možností určení priority nebo šířky pásma zvoleného provozu
- automatické řízení kvality služeb (QoS) pro hlas a video
- Podpora MU-MIMO (Multi-User MIMO) - multi-user multiple input/multiple output
- SU-MIMO (Single-User MIMO) min. 1300Mb, MU-MIMO min. 850 Mb
- Detekce cizích přístupových bodů zjištěných v LAN i v radiofrekvenčním pásmu
- Virtuální, vysoce dostupný kontroler obsažený ve firmware každého přístupového bodu. Umožňuje kompletní centrální správu WiFi infrastruktury a řízení jejího provozu včetně roamingu klientů.
- plná podpora CLI, SSH, SNMP 1-3, syslog, web rozhraní
- automatické dynamické přidělování kanálů a řízení výkonu přístupových bodů pro vyrovnané pokrytí a minimalizaci interference
- záruka 60 měsíců v režimu NBD, odeslání náhradního zařízení max. následující pracovní den po nahlášení závady, včetně nároku na aktuální verze firmware

Stojanový rozvaděč 42U 1x

- Provedení: **Stojanový rozvaděč 19" 42U (š)800x(h)1000 rozebíratelný př.i zad.dv.síto černý**
- Konstrukce rozvaděče: ocelový svařovaný skelet s odnímatelnými krycími panely, rozebíratelný přední i zadní dveře síto
- Rozměr: 42U, šířka 800mm, hloubka 1000mm
- Nosnost: 400 kg

- Příslušenství: Rack bude dále vybaven Patch panelem 24p. CAT6 UTP 3x8p LSA 1U horní zářez, 19" vyvazovací panel 1U, háček 60x30mm zacvakávací, 4x Prodlužovacím přívodem 230V, 5m, 6 zásuvek + vypínač a montážní sadou M6 (50x šroub, matice, podložka)
- Záruky 24 měsíců

Nástěnný rozvaděč 12U 3x

- Provedení: **Nástěnný rozvaděč RUA 12U/500mm odn.boč+skl.dv.černý**
- Konstrukce rozvaděče: Jednodílný svařovaný rozvaděč s odnímatelnými bočnicemi, IP30, s nosností 30 kg
- Rozměr: 12U, šířka 600mm, hloubka 500mm
- Nosnost: 30 kg
- Příslušenství: Rack bude dále vybaven Patch panelem 24p. CAT6 UTP 3x8p LSA 1U horní zářez, 19" vyvazovací panel 1U, háček 60x30mm zacvakávací, Prodlužovacím přívodem 230V, 5m, 6 zásuvek + vypínač a montážní sadou M6 (50x šroub, matice, podložka)
- Záruka 24 měsíců

Bezpečnostní certifikát

- Hvězdičkový (tzv. wildcard) certifikát veřejné certifikační autority pro zabezpečení služeb publikovaných do internetu. Kořenový certifikát certifikační autority musí být standardně obsažen v běžných desktopových a mobilních operačních systémech a být automaticky aktualizován v rámci aktualizace operačního systému.
- Záruka: 36 měsíců

K3 – Centrální logování

Monitorovací a logovací systém

- Vlastní řešení společnosti AutoCont **AC LOG System Open Source** založené na open-source produktech, doplněné a upravené pro sběr, ukládání a správu provozních a bezpečnostních informací a událostí ze sledovaných systémů
- Základní funkce: Systém pro sběr, ukládání a správu provozních a bezpečnostních informací a událostí ze sledovaných systémů
- Protokoly sběru logů: syslog, TCP, UDP, HTTP, AMQP, JSON
- Sběr síťových toků: netflow či kompatibilní dle nabízeného firewallu a centrálního přepínače
- Zdroje logů: REST API, textové soubory, Radius, Active Directory, MS SQL databáze, Windows Event Log - včetně rozšířených "Applications and Services Logs", síťové prvky - syslog a netflow, ostatní aktivní prvky - syslog, SNMP trap
- Parsování logů: Integrovaný nástroj pro parsování logů. Možnost nahrání části logu, online vytváření parseru a snadné testování výsledku. Podpora vytváření opakovaně použitelných vzorků - např. definice IP adresy regulárním dotazem apod.
- Retence: Uchovávání logů min. 6 měsíců, automatická retence logů a indexů
- Geolokace: Podpora automatické doplňování logů o informaci o lokalitě podle IP adresy
- Normalizace logů: Sjednocení názvů shodných dat z různých zdrojů logů např. pro snadné vyhledávání napříč zdroji
- Rozšíření logů: Podpora rozšíření logů o vlastní statické a dynamické (kalkulované) položky integrovaným nástrojem
- Rozšiřitelnost: Podpora snadného rozšíření funkčnosti pomocí plug-inů nebo modulů
- Bezpečnost: Podpora šifrované komunikace se zdroji (SSL apod.), ověřování zdrojů (TLS apod.)
- Výkon: 500 EPS (event per second), 5000 FPM (flows per minute)
- Dashboards: Uživatelské vytváření dashboardů (pracovních desek) včetně možnosti využití grafických prvků (grafy, mapy, histogramy apod.) i strukturovaných dat (tabulek)
- Export dat: Export dat do csv a/nebo xls - min. výsledky hledání
- Kanály: Možnost vytváření kanálů - datových sad či toků - na základě pravidel (logických podmínek) a to i napříč různými zdroji. Podpora dalšího zpracování - tvorba alarmů, zobrazení na dashboardu, online odesílání do nadřazeného systému apod.
- Alerty, notifikace: Podpora vytváření alertů - překročení okamžitých či kumulovaných hodnot, zasílání upozornění
- Active Directory: integrace s Active Directory pro ověřování uživatelů, nastavení oprávnění min. administrátor a operátor
- Vyhledávání: Rychlé a intuitivní vyhledávání v záznamech napříč všemi zdroji i při velkých objemech dat (řády TB). Jednoduchý dotazovací jazyk. Rychlá vyhledávání či filtrování bez tvorby dotazů - např. výběrem v kontextovém menu vybraného pole uloženého záznamu
- Ovládání: Intuitivní grafické rozhraní
- Kompatibilita: Podpora provozu v prostředí nabízené serverové virtualizace
- Ukládání dat: do databáze, případná databázová licence je součástí dodávky
- Výstupy: Možnost výstupů do nadřazeného systému pro účely vzdáleného expertního dohledu. Zabezpečený přenos vhodným protokolem
- Záruka: 60 měsíců včetně poskytnutí opravných verzí

AC Identity management systém SW

- Základní funkce: IDM (dále IDM nebo Systém) bude udržovat a spravovat identity a organizační strukturu organizace – třídy, učitelský sbor, administrativa atd. Spravované identity budou sloužit jako referenční identity pro ostatní vnitřní i vnější informační systémy. Identity budou ukládány v databázi.
- Licence: Poskytnutá licence umožní nasazení a provoz IDM bez omezení na počet uživatelů, spravovaných identit a napojených systémů. Nejsou přípustná žádná další omezení omezující obvyklé nasazení a provoz s ohledem na charakter organizace Zadavatele (počet záznamů, velikost databází atd.).

Předpokládaný počet uživatelů je do 500.

- Škálovatelnost: Systém musí umožnit zvyšování výkonu (zlepšování odezvy) rozložením komponent Systému na více serverů – minimálně oddělení rolí (serverů) uživatelského rozhraní od výkonu integračních a provozních úloh.
- Evidence aplikací a rolí: Integrovaný registr aplikací a informačních systémů (souhrnně IS) a jejich uživatelských rolí včetně možnosti importu rolí přes webové služby.
- Uživatelské role: Integrovaná správa uživatelských rolí, včetně zařazení uživatele do odpovídající role v příslušných IS.
- Historizace: Vestavěná detailní databázové historizace pro evidenci změn identit včetně referenčních objektů a vazeb mezi nimi. Historizace poskytne data v libovolném časovém okamžiku – aktuálním nebo zpětně v minulosti.
- Automatizace: Podpora intuitivní tvorby pravidel v grafickém prostředí pro automatické vytváření uživatelských účtů, začleňování uživatelů do skupin a přiřazování aplikačních rolí uživatelům na základě libovolných atributů identity a přidružených referenčních objektů (organizační jednotka, aplikační role, pracovní pozice atd.).
- Logování: Systém bude poskytovat auditní logy pro požizovaný logovací a monitorovací systém
- Logování systému: Systém obsahuje logování min. následujících typů událostí:
 - události systému (aplikační log)
 - změny entit evidovaných systémem a změny konfigurace systému (auditní log)
 - synchronizace s napojenými systémy (synchronizační log)
 - odeslané notifikace a upozornění (notifikační log)
- Správa identit: Systém bude spravovat organizační strukturu obsahující interní a externí identity jako samostatné větve struktury.
- Podpora eIDAS: Systém umožní implementaci procesů a rozhraní, která jsou vyžadována v Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.
- Požadavky na portál: IDM bude obsahovat webový portál (dále jen Portál), který bude sloužit jako hlavní rozhraní pro uživatele i správce pro přístup k datům, funkcím, správu a konfiguraci Systému.
- Správa referenčních objektů: Portál bude umožňovat přehlednou správu samostatných identifikovatelných objektů – referenčních objektů, na které se identity mohou odkazovat: min. pracovní pozice, organizační jednotka, skupina, aplikace, skupina aplikací, aplikační role.
- Referenční objekty: Systém umožní přidávání a správu dalších typů referenčních objektů, a to i v průběhu správy konkrétní identity s možností okamžitého použití referenčního objektu u spravované identity
- Zabezpečení referenčních objektů: Systém umožní nastavení samostatných nezávislých administrátorských oprávnění pro správu jednotlivých referenčních objektů
- Rozšiřující atributy: Systém umožní dodatečné rozšiřování identit a referenčních objektů o další atributy a zajistí publikaci těchto nových atributů externím aplikacím prostřednictvím rozhraní webových služeb IDM.

- Přehledné zobrazení: Portál umožní grafické zobrazení a současné vyhledávání identit / uživatelských účtů ve stromové organizační struktuře a prohledávání organizační struktury včetně pracovních pozic až do úrovně jednotlivých uživatelských účtů (identit).
- Vyhledávání – diakritika: Portál bude umožňovat vyhledávat i bez diakritiky (např. zadání Cizova vyhledává i Čížová apod.)
- Obrázky: Systém umožní k jednotlivým účtům (identitám) přikládat obrázky – fotografie.
- Ochrana proti chybám: Systém bude obsahovat mechanismus zabránění hromadným změnám z důvodu případných chybných vstupních dat (např. z personálního systému), aby nedošlo k hromadným nežádoucím změnám (například smazání objektů v Active Directory apod.).
- Aktivní uživatelé: Systém bude obsahovat přehled uživatelů aktuálně pracujících s Portálem
- Granularita oprávnění: Oprávnění přidělována uživatelům a správcům bude možné definovat a přidělovat pro jednotlivé části systému (identity, referenční objekty, notifikací, synchronizací, konfigurace systému, webové služby atd.). U jednotlivých částí bude možnost definovat akce, které může uživatel s přidělenými oprávnění v konkrétní části IDM provádět.
- Časová omezení: IDM bude umožňovat přiřazení rolí konkrétní identitě, pracovní pozici, skupině a organizační jednotce včetně možnosti nastavení data a času vypršení platnosti přiřazení. Po vypršení platnosti přiřazení IDM rolí přiřazenému objektu automaticky odebere.
- Vícenásobné vazby: Možnost přiřazení identit k pracovním pozicím ve vazbě M:N. Identita může být v IDM evidována na více pracovních pozicích současně a současně na pracovní pozici může být evidováno více identit.
- Přehled rolí: Možnost zobrazení přidělených rolí k jednotlivým identitám s přehledným rozlišením rolí navázaných na pracovní pozici, rolí navázaných na identitu, rolí navázaných na organizační jednotku, rolí navázaných na skupinu a delegovaných role.
- Přehled dědičností: IDM umožní evidenci a přehledné souhrnné zobrazení všech rolí včetně informace, odkud uživatel roli zdědil (z organizační jednotky, pracovní pozice, skupiny) nebo zda má nějakou roli od někoho delegovanou.
- Skupiny: IDM bude obsahovat správu skupin s možností začleňovat více skupin do sebe, přiřazovat do skupin jednotlivé uživatele i pracovní pozice.
- Delegování oprávnění: Možnost delegování administrátorských práv.
- Obnovení hesla: IDM bude obsahovat samoobslužné uživatelské rozhraní pro reset hesla jednotlivých účtů daného uživatele. Zasílání kódů pro reset hesla danému uživateli musí být možnou provádět pomocí SMS (tj. IDM musí být možné na SMS bránu či službu napojit). Rozhraní musí umožnit i běžnou změnu hesla (bez resetu).
- Individualizace: IDM umožní uživatelům individuálně nastavit vlastní zobrazení rozhraní - min. zobrazení / skrytí sloupců u všech seznamů, počet zobrazených záznamů na stránku (buď několik přednastavených hodnot nebo možnost ručního nastavení) - vždy pro každý seznam samostatně.
- Upozornění: IDM zajistí zasílání konfigurovatelných emailových upozornění min. pro následující události: vytvoření a změna identity, referenčního objektu (pracovní pozice, organizační jednotka, skupina, aplikace, skupina aplikací, aplikační role atd.), problém při synchronizaci, vypršení hesla v Active Directory, vypršení platnosti certifikátu.
- Včasná upozornění: Upozornění na vypršení časových termínů musí být možno zasílat v předstihu. Velikost předstihu (např. 10 dnů) musí být možno konfigurovat pro každý typ upozornění samostatně.
- Šablony upozornění: Šablony upozornění umožní definovat příjemce, předmět a obsah upozornění. U upozornění vázaného k identitám musí být možné nastavovat různé příjemce pro různé části organizační struktury (např. odbor, oddělení) apod. Šablony musí umožnit vložit do obsahu upozornění libovolný atribut identity a/nebo referenčního objektu.
- Kontext upozornění: Pro zasílání jednotlivých typů upozornění bude možno konfigurovat kontext, resp. podmínky, za jakých bude upozornění zasláno. V konfiguraci bude možné využít atributů identit a referenčních objektů. Příklad: notifikace budou generovány pouze pro identity v konkrétních uvedených skupinách, které mají uvedenu konkrétní aplikační role a konkrétní atribut atd.
- Logování: Veškeré změny vyvolané požadavky uživatele a administrátorů/správce IDM budou provedeny transakčně. Budou logovány tak, aby bylo možné zpětně prokázat co, kdo a kdy změnil v

identitách a referenčních objektech i v administraci a konfiguraci IDM. Záznam v logu bude obsahovat původní i novou hodnotu.

- Důvěryhodnost logování: Veškeré požadavky na změny v IDM bude možné zadávat výhradně prostřednictvím Portálu. Není přípustné realizovat požadavky ručními změnami textových souborů jako XML, CSV, atd. z důvodu zajištění úplného logování všech změn jednotlivých konfigurovaných parametrů IDM.
- Auditní report: IDM umožní export auditního reportu z údajů o identitách uložených v IDM, a to i historických. Auditní reporty budou minimálně ve formátu XML nebo CSV a budou obsahovat souhrnné zobrazení daných uživatelů (identit) a jejich rolí v IS napojených na IDM, přiřazených skupin ve vybraném časovém okamžiku od aktuálního času do minulosti.
- Auditní report – výběr: Identity pro generování auditního reportu musí být možné vybrat (filtrovat) dle libovolných atributů identity včetně přidružených referenčních objektů.
- Reporty uživatelů: Vestavěné reporty obsahující uživatele s přímo přiřazenými aplikačními rolemi a s aplikačními rolemi delegovanými od jiných uživatelů. Reporty budou exportovatelné do CSV souboru.
- Reporty – historie: Automatické ukládání vygenerovaných reportů s možností pozdějšího zobrazení či stažení.
- Webové služby (WS): IDM bude poskytovat rozhraní webových služeb pro napojení dalších systémů s možností konfigurace v Portálu.
- Standardy WS: Webové služby IDM budou definované v rozšířeném standardu WSDL a podporovat protokol SOAP.
- Bezpečnost WS: Konfigurace webových služeb umožní konfigurovat přístup pro volání jednotlivých vybraných služeb pro každý odpovídající systémový účet samostatně.
- Logování WS: Volání webových služeb bude logováno a bude možné je zobrazit v prostředí Portálu
- Služby rozhraní WS: Rozhraní bude poskytovat minimálně následující služby:
 - Získání organizační struktury
 - Získání hierarchie pracovních pozic
 - Získání seznamu identit
 - Získání nadřízené osoby pro daného zaměstnance
 - Získání seznamu aplikačních rolí
 - Získání seznamu uživatelů dané aplikace
 - Zápis seznamu aplikačních rolí do IDM
 - Zápis a změna identit
- Synchronizace: Ruční i automatické spuštění synchronizací s propojenými systémy.
- Synchronizace – simulace: Spuštění synchronizací i v simulačním režimu pro ověření dopadu reálného spuštění bez ovlivnění produkčních dat a napojených systémů. Simulační logy budou zobrazitelné v Portálu.
- Simulace – průběh: Zobrazení jednotlivých stavů průběhu synchronizace bude k dispozici v přehledné grafické podobě.
- Synchronizace – režimy: Pro napojení na jednotlivé systémy a implementaci jejich synchronizací s IDM umožní IDM u každého systému využít více režimů synchronizací (za předpokladu podpory napojovaného systému):
 - Plná synchronizace – prochází všechny objekty v IDM a synchronizuje je s objekty daného systému
 - Změnová synchronizace – synchronizuje vždy jen změny od poslední spuštěné synchronizace
 - Simulační synchronizace – synchronizace vytvoří report očekávaných změn v napojeném systému pro provedení ostré synchronizace. Report změn bude evidován jako pohled nebo přehledná souhrnná tabulka.
 - Historie běhu synchronizací – jednotlivé běhy synchronizací budou zaznamenány v historii dostupné v Portálu. Historie plné synchronizace bude obsahovat odkazy na objekty, které byly synchronizovány a log, co bylo u těchto objektů změněno v synchronizovaném systému. V případě změnové synchronizace pak bude v historii dále informace o události, která změnovou synchronizaci vyvolala.
- Synchronizace – správa: Vestavěná správa jednotlivých synchronizací včetně nastavení připojení na synchronizované systémy, nastavení plné a změnové synchronizace, počet změn, které je možné

zpracovat, nastavení časového intervalu spouštění, nastavení intervalu odstávky. Správa bude součástí Portálu.

- Obecný konektor: Pro správu identit nenapojených aplikací a testování. Konektor simuluje aplikaci, požadavky na změny nastavení v aplikaci zasílá e-mailem správci aplikace. Podpora zpětné vazby – správce v IDM potvrzuje provedení požadavků pro účely logování
- Aplikační konektory: IDM bude spravovat identity a řídit oprávnění v dále vyjmenovaných systémech. V těchto systémech bude IDM vytvářet, aktualizovat, vytvářet uživatele a nastavovat jim oprávnění k rolím.
 - Microsoft Active Directory
 - Microsoft Office 365 nebo GSuite
- Zdrojový systém: IDM bude napojeno na školský informační systém Bakaláři. Ze systému Bakaláři budou načítány údaje o organizační struktuře, osobách a tyto údaje budou pro IDM sloužit jako zdrojové
- Záruka: 60 měsíců včetně nároku na opravné a nové verze