FUNKČNÍ A TECHNICKÉ POŽADAVKY

k veřejné zakázce

Dodávka HW, SW a služeb v oblasti infrastruktury datových center

Ev.č.: 499467

zadávané v otevřeném nadlimitním řízení dle zákona č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů (dále jen „ZVZ“)

Zadavatel veřejné zakázky:

Česká republika – Ministerstvo práce a sociálních věcí

se sídlem Na Poříčním právu 1/376, 128 01 Praha 2

IČO: 00551023

(dále jen „**zadavatel**“ nebo „**MPSV**“)

Osoba oprávněná zastupovat zadavatele
Ing. Iva Merhautová, MBA, náměstkyně ministryně pro informační a komunikační technologie

Zástupce zadavatele
Kontaktní osobou ve věcech souvisejících se zadáváním této veřejné zakázky je MT Legal s.r.o., advokátní kancelář, Karoliny Světlé 25, 110 00 Praha 1, e-mail: vz@mt-legal.com. Kontaktní osoba zajišťuje veškerou komunikaci zadavatele s dodavateli (tím není dotčeno oprávnění statutárního orgánu či jiné pověřené osoby zadavatele) a je v souladu s ust. § 151 ZVZ pověřena výkonem zadavatelských činností v tomto zadávacím řízení. Kontaktní osoba je pověřena také k přijímání případných námitek dodavatelů dle ust. § 110 ZVZ.

1 POPIS 4
1.1 Úvod 4
1.2 Informační systémy 4
2 Předmět plnění 8
3 Základní požadavky na dedikovaná datová centra 9
3.1 Základní požadavky na DDC 9
3.1.1 Požadavky na licenční zajištění 11
3.1.2 Požadavky na hardware a software 12
3.1.3 Požadavky na záruční lhůty a dostupnost náhradních dílů 12
3.1.4 Požadavky na energetickou úspornost 12
3.1.5 Požadavky na kompatibilitu 12
3.2 Umístění Datových center 13
3.3 Požadavky na Datové centrum A nebo Datové centrum B 14
3.3.1 Požadavky na komunikační infrastrukturu 18
3.3.2 Požadavky na fyzické servery virtualizační vrstvy 24
3.3.3 Požadavky na samostatné servery s vlastním diskovým prostorem (TYP C) 28
3.3.4 Požadavky na disková pole 29
3.3.5 Zálohování a dlouhodobé ukládání dat 34
3.3.6 Požadavky na datové rozvaděče a podružný materiál 39
3.4 Monitorovací systém DDC 39
3.4.1 Požadavky na hardware 43
3.5 Požadavky na funkcionalitu Datových center 43
3.5.1 Požadavky na virtualizační clustery 45
3.5.2 Požadavky na virtuální servery 47
3.6 Dohledové centrum 48
3.6.1 Požadavky na dohledové servery 51
3.6.2 Požadavky na koncové počítače dohledového centra 51
3.6.3 Požadavky na zajištění vzdáleného přístupu 52
3.7 Dodávka hardware a software 52
3.8 Implementace 53
3.8.1 Instalace a zprovoznění 53
3.8.2 Ověřovací provoz Datového centra A 54
3.8.3 Ověřovací provoz Datového centra B 54
3.8.4 Akceptace DDC 55
3.9 Ostatní činnosti 55
3.9.1 Konzultační činnosti 55
3.9.2 Technologické činnosti 55
3.10 Technická a systémová dokumentace 57
3.10.1 Technický projekt 57
3.10.2 Bezpečnostní projekt 58

3.10.3 Ostatní dokumentace 58
3.10.4 Požadavky na bezpečnost 59
3.11 Požadavky na spolupráci s provozovateli systémů/aplikací 60
3.12 Požadavky na spolupráci s poskytovatelem služeb podpory provozu současných datových center 60
3.13 Požadavky na Služby – Katalog služeb 60
3.13.1 Definice pojmů 60
3.13.2 Definice služeb, komponent a částí 64
4 Požadavky na součinnost zadavatele 84
4.1.1 Součinnost zadavatele pro analýzu a návrh 84
4.1.2 Součinnost zadavatele pro testování 84
4.1.3 Součinnost zadavatele pro nasazení 84
4.1.4 Součinnost zadavatele pro školení 85
4.1.5 Součinnost pro projektové řízení 85
5 Použité termíny 85

1 POPIS

1.1 Úvod

Ministerstvo práce a sociálních věcí v současné době provozuje informační systémy ve tyřech stávajících datových centrech. Dvě datová centra obsahují provoz agendových informačních systémů a dalších návazných evidencí, další dvě zajišťují infrastrukturní služby pro rezort. Provoz stávajících datových center zajištuje několik dodavatelů, kdy každý má na starost určitý logický celek stávajících datových center.

Rozvoj stávajících datových center byl postupný a reflektoval aktuální potřeby resortu MPSV, neboť dlouhodobý koncept rozvoje rezortních informačních technologií MPSV nebyl k dispozici. Z výše uvedených důvodu jsou v rámci stávajících datových center provozovány různé platformy a různé technologie, kde je nemožné, případně velmi nákladné zajistit další provoz a údržbu.

1.2 Informační systémy

Ministerstvo práce a sociálních věcí provozuje dle příslušné legislativy "Jednotný informační systém práce a sociálních věcí" (dále také jako "JISPSV"), který zajišťuje podporu výkonu agend resortu a dalších návazných evidencí. Resort MPSV a jeho agendy jsou naprosto klíčovými službami státu, jež pro svoje klienty představují mnohdy naprostou existenční nutnost. V první řadě je tedy povinností resortu tyto služby zajistit, a to řádným výkonem souvisejících agend veřejné správy.

Pro výkon svých agend využívá resort zejména JISPSV, jež provozuje na základě § 4a, Zákona č. 73/2011 Sb., o Úřadu práce ČR a na základě jednotlivých agendových zákonů. JISPSV je informačním systémem veřejné správy dle Zákona č. 365/2000 Sb., o informačních systémech veřejné správy a je agendovým informačním systémem dle Zákona č. 111/2009 Sb., o základních registrech.

Ministerstvo je správcem Jednotného informačního systému práce a sociálních věcí, jehož obsahem jsou údaje nezbytné k plnění úkolů ministerstva a Úřadu práce v oblasti státní sociální podpory, pomoci v hmotné nouzi, příspěvku na péči, dávek pro osoby se zdravotním postižením, sociálně-právní ochrany dětí, státní politiky zaměstnanosti a ochrany zaměstnanců při platební neschopnosti zaměstnavatele. Jednotný informační systém práce a sociálních věcí může ministerstvo a Úřad práce využít rovněž za účelem získání potřebných údajů nezbytných pro výplatu a kontrolu vyplácení dávek nebo podpory v nezaměstnanosti, podpory při rekvalifikaci nebo kompenzace. Součástí Jednotného informačního systému práce a sociálních věcí je rovněž Standardizovaný záznam sociálního pracovníka vedený podle zákona o pomoci v hmotné nouzi a zákona o sociálních službách.

Ministerstvo práce a sociálních věcí hodlá formou více veřejných zakázek poptat a implementovat nový JISPSV tak, aby odpovídal potřebám resortu a potřebám podpory výkonu agend, aby byl v souladu s moderními principy eGovernmentu v ČR (jak jsou definovány Ministerstvem vnitra ČR a hlavním architektem) a aby tímto způsobem byly vyřešeny stávající problémy a nedostatky nekonsolidovaného řešení výkonu některých agend. MPSV tak činí na základě modulové architektury nového řešení JISPSV, a bude tedy poptávat jednotlivé části JISPSV (ať už jako informační systémy, evidence, či další části) v několika navazujících a zároveň logických celcích.

Prvním celkem je pak skupina zakázek v přímém vztahu k systémům podporujících činnost MPSV a ÚP v oblasti vykonávaných agend. Jedná se o tyto zakázky:

1. *Jednotný informační systém práce a sociálních věcí – IS ZAMĚSTNANOST*
   Předmětem zakázky je dodání a implementace a provoz a podpora systémů a evidencí oblastí pro podporu výkonu agend zaměstnanosti. Jedná se o Informační systém o zaměstnanosti. Tento informační systém podporuje agendy v oblasti zaměstnanosti a trhu práce, jak jsou popsány dle Zákona č. 435/2004 Sb., o zaměstnanosti a související evidence.
2. *Jednotný informační systém práce a sociálních věcí – IS DÁVKY*
   Předmětem je dodání a implementace informačních systémů jednotlivých agend v oblasti dávek dle příslušné legislativy:
   a. *Informační systém o dávkách státní sociální podpory* - tento informační systém je provozován dle Zákona č. 117/1995 Sb., o státní sociální podpoře a sdružuje evidence a údaje pro rozhodování a výplatu dávek státní sociální podpory. Předmětem je dodání tohoto informačního systému, a to včetně migrace stávajících dat a zajištění souvisejících procesů.
   b. *Informační systém pomoci v hmotné nouzi* - tento informační systém je provozován na základě Zákona č. 111/2006 Sb., o pomoci v hmotné nouzi a vede údaje a evidence související s výkonem agendy a činností v tomto zákoně. Předmětem je dodání tohoto informačního systému, a to včetně migrace stávajících dat a zajištění souvisejících procesů.
   c. *Informační systém o příspěvku na péči* - jedná se o jeden z informačních systémů provozovaných na základě Zákona č. 108/2006 Sb., o sociálních službách, jež slouží pro výkon agend a činností souvisejících s příspěvkem na péči. Předmětem je dodání tohoto informačního systému, a to včetně migrace stávajících dat a zajištění souvisejících procesů.
   d. *Registr poskytovatelů sociálních služeb* - jedná se o jeden z informačních systémů provozovaných na základě Zákona č. 108/2006 Sb., o sociálních službách, jež slouží pro podporu agend a činností souvisejících s poskytovateli sociálních služeb, s dotačními programy a financováním, výkaznictvím v této oblasti a inspekcí v oblasti sociálních služeb. Předmětem je dodání tohoto informačního systému, a to včetně migrace stávajících dat a zajištění souvisejících procesů.
   e. *Informační systém o dávkách pro osoby se zdravotním postižením* - tento informační systém je provozován na základě Zákona č. 329/2011 Sb., o poskytování dávek osobám se zdravotním postižením a jeho agend a slouží pro podporu agend a činností souvisejících s příspěvkem na mobilitu a s příspěvkem na zvláštní pomůcku a s posuzováním a vydáváním průkazu osob se zdravotním postižením. Předmětem je dodání tohoto informačního systému, a to včetně migrace stávajících dat a zajištění souvisejících procesů.
   f. *Evidence držitelů průkazů osoby se zdravotním postižením* - evidence obsahuje údaje o držitelích průkazu osoby se zdravotním postižením na základě Zákona č. 329/2011 Sb., o poskytování dávek osobám se zdravotním postižením a rozsahu mimořádných výhod dle druhu průkazu. Existují orgány veřejné moci, jež takové údaje mohou od MPSV získávat a jež je potřebují k některým činnostem. V budoucnu se navíc objeví potřeba získávání těchto údajů k prověření nároku na mimořádné výhody pro držitele těchto průkazů i pro fyzické a právnické osoby poskytující služby, jejichž zvláštní režim poskytování pro zdravotně postižené je stanoven. Předmětem je dodání tohoto informačního systému, a to včetně migrace stávajících dat a zajištění souvisejících procesů.
   g. *Informační systém sociálně-právní ochrany dětí* - tento informační systém je provozován pro agendy Zákona č. 359/1999 Sb., o sociálně-právní ochraně dětí. Obsahuje evidence a slouží pro podporu agend a činností v tomto zákoně, a to zejména v souvislosti s pěstounskou péčí a náhradní péčí o dítě. Předmětem je dodání tohoto informačního systému, a to včetně migrace stávajících dat a ajištění souvisejících procesů.

3. *Integrovaná podpůrná a provozní data JIS*

   Předmětem je dodání a implementace a vazby některých klíčových částí nutných pro podporu fungování celého řešení JISPSV, a to zejména v souvislosti s nutností naplnění legislativních požadavků souvisejících s principy eGovernmentu a s vazbami na činnosti, které nejsou primárně agendami dávkového typu:

   a. *Evidence subjektů a napojení na registry* - je základní kmenovou evidencí osob – jak fyzických osob a jejich vazeb, tak právnických osob a jejich vazeb na osoby fyzické. Podle Zákona č. 111/2009 Sb., o základních registrech musejí i orgány v oblasti sociální péče jako orgány veřejné moci využívat referenční údaje ze základních registrů a nesmějí požadovat jejich další doložení. Evidence fyzických osob bude provázána s Registrem obyvatel (ROB) a Informačním systémem evidence obyvatel (ISEO) a Cizineckým informačním systémem (CIS), jako se základními systémy obsahujícími údaje o entitách fyzických osob a jejich základních vazbách. Pro účely sociální oblasti je však nezbytné udržovat také historii údajů a vazeb jednotlivých fyzických osob, a to jak v návaznosti na agendy v naší gesci, tak v návaznosti na další věci (zákonný zástupce, opatrovník osoby omezené na způsobilosti apod.). Základní údaje o fyzických osobách a jejich vazbách budou jednotlivé informační systémy JISPSV čerpat z evidence subjektů. Evidence právnických osob bude provázána s údaji v Registru osob (ROS) o právnických osobách a o určitých vazbách na fyzické osoby (jednatel apod.), a to pro účely všech resortních agend a evidencí (třeba v oblasti zaměstnanosti, poskytovatelů sociálních služeb apod.). Existují ale i právnické osoby, které nejsou vedeny v ROS a tyto osoby bude vést evidence subjektů také. Evidence subjektů bude zajišťovat aktuálnost údajů ze základních registrů formou notifikací a aktualizací změn referenčních a dalších údajů.

   b. *Sdílené a kompozitní služby* - Tato část bude zajišťovat bod rozhraní pro poskytované služby orgánům veřejné moci a fyzickým a právnickým osobám ve třech základních módech - kompozitní služby ISZR, služby poskytované třetím stranám na základě oborových zákonů MPSV, služby poskytované třetím stranám na základě jiných práv.

   c. *Evidence případů* - Evidence případů bude sloužit k jednoduché evidenci informací o pravomocných rozhodnutích kupříkladu o výplatách jednotlivých dávek. Subjekty budou identifikovány v Evidenci subjektů a jednotlivé informační systémy budou do této Evidence případů zapisovat informace o platných rozhodnutích, jež jsou v danou chvíli v právní moci, ale také o rozhodnutí historických. Evidence případů řeší situace, kdy legislativa a související procesy vyžadují znalost toho, zda subjekt pobírá nějakou dávku, či zda čerpá nějakou službu sociálního systému (třeba zda je v pobytovém zařízení sociálních služeb a tím pádem má omezená práva v souvislosti s dávkami pro osoby se zdravotním postižením). Místo složitého ručního dohledávání či dotazování do všech modulů i s historickými konsekvencemi (neboť v mnohých případech je nutno znát tyto skutečnosti s historickou znalostí několika měsíců předcházejících příslušnému řízení), se využije tato evidence. Tím se zabrání zbytečné nutnosti předávání údajů z mnoha systémů a naopak se ztransparentní, “co kdo a na základě čeho uvidí” a pro jaký účel.

   d. *Číselníky a datové prvky* - obsahuje číselníky a společné datové prvky, jež jsou využívány v dalších modulech a částech JISPSV. Je-li určitý datový prvek řízen číselníkem možných hodnot, je tento číselník spravován zde centrálně a daná součást jej povinně čerpá i s hodnotami z této části.

   e. *Agendy právních služeb* - tato část zajišťuje podporu pro agendy, jež nejsou primárními agendami resortu, ale jež s výkonem agend a činností v resortu souvisejí a mají nějaký vztah k datům vedeným v JISPSV – respektive k osobám vedeným v evidencích. Například se týká agend exekucí, srážek z dávek, insolvencí a dalších. Předmětem je dodání informačního systému podporujícího tyto agendy a činnosti dle jejich rozsahu a procesů.

4. *Integrace a provoz JIS*

   Předmětem zakázky je:

   a. *Implementace technologií Enterprise Service Bus* na platformě Microsoft, jejichž licencemi zadavatel disponuje.

   b. *Implementace technologií Enterprise Document Storage a Data Content Storage* na platformě Microsoft, jejichž licencemi zadavatel disponuje.

   c. *Koordinace a implementace referenčních a integračních rozhraní* přes ESB pro integraci jednotlivých informačních systémů a částí JIS.

   d. *Zajištění integrace do JIS* pro následující moduly - identity management a správa entit, certifikační autorita a správy certifikátů, auditování a logování, identity management a autentifikace a autorizace, certifikační autorita a správa prostředků důvěry, modul pro audity a logy, podpora tvorby a implementace metodik (formou workflow v rámci DS), modul školení uživatelů a eLearningu, systém podpory uživatelů, systém řízení činností, monitoring a dohled nad celým systémem formou zajištění implementace a integrace příslušných dohledových nástrojů nad celým systémem a nad ESB.

2 PŘEDMĚT PLNĚNÍ

Předmětem plnění této veřejné zakázky je dodávka hardware a software souvisejícího s nově budovanou infrastrukturou DC MPSV, včetně služeb souvisejících se zprovozněním, konfigurací, instalací, nasazením dodaného hardware a software a zajištěním služeb podpory provozu nově zřizovaných dedikovaných datových center MPSV (dále jen společně jako „DDC“, nebo samostatně také jako „Datové centrum A“ a „Datové centrum B“).

Předmět plnění této veřejné zakázky zahrnuje následující části:

- dodávka hardware a software,
- implementace,
- vytvoření a dodání technické a systémové dokumentace,
- poskytování služeb servisní, technické a systémové podpory dodávané Infrastruktury,
- konzultace - poskytování služeb IT specialistů.

3 ZÁKLADNÍ POŽADAVKY NA DEDIKOVANÁ DATOVÁ CENTRA

3.1 Základní požadavky na DDC

MPSV požaduje zřízení dvou plně funkčních a na sobě nezávislých dedikovaných datových center s centralizovaným managementem a následným zajištěním jejich provozu na dobu 4 let. DDC budou umístěna v prostorách určených zadavatelem.

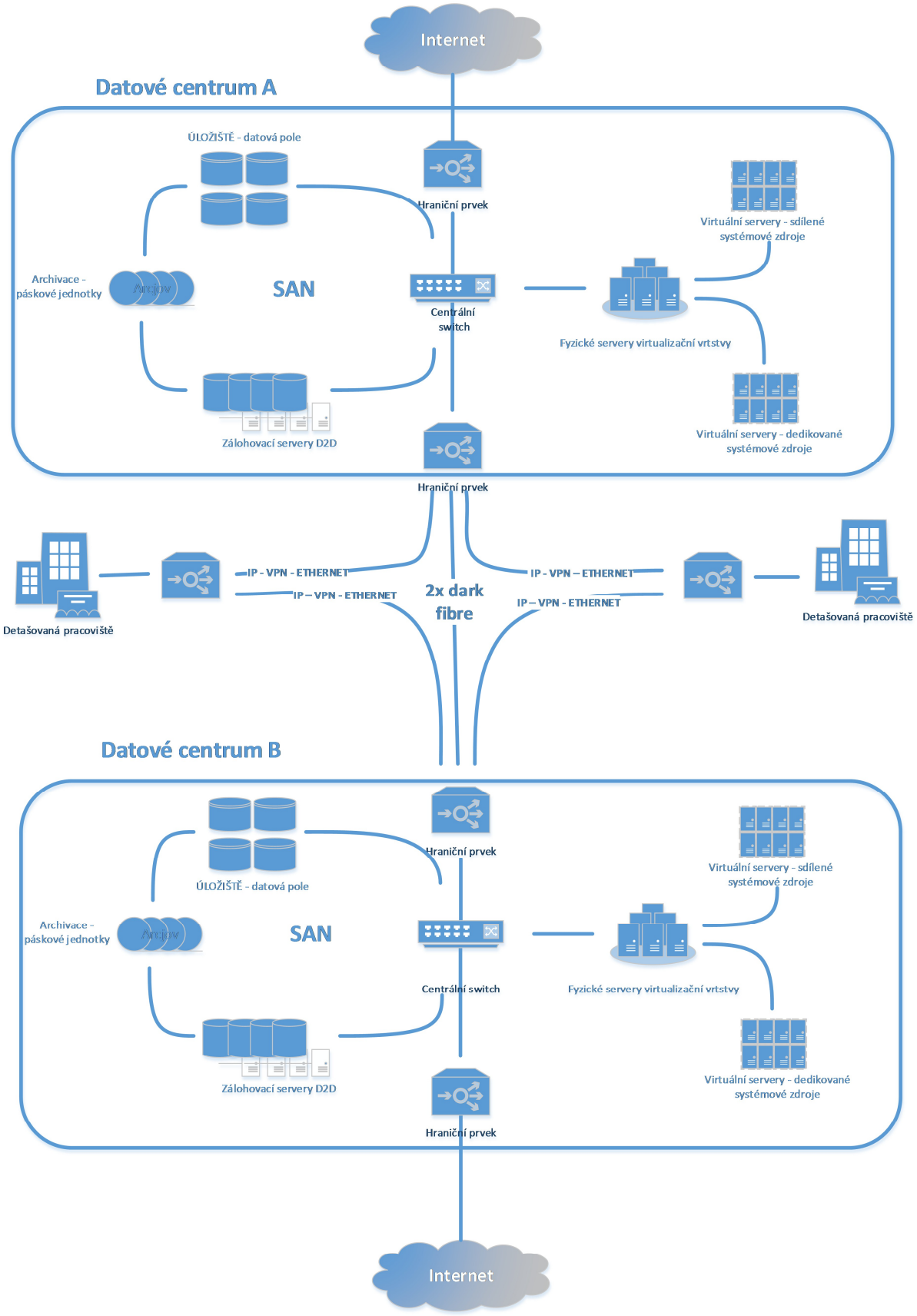
DDC budou sloužit pro provozování všech informačních systému, aplikací a jiných podpůrných systémů zadavatele v režimu vysoké dostupnosti (zejména se jedná o infrastrukturní služby -Active Directory, DNS, DHCP, služby elektronické pošty, DMS, PBX, informační systémy JIS a jiné systémy databázové, aplikační a prezentační vrstvy). Součásti DDC bude řešení pro jeho zálohování i monitoring DDC.

Základní požadavky na DDC jsou:

- architektura typu x86 (podpora 64bit),
- energetická úspornost,
- modularita (SAN, komunikační infrastruktura, virtualizační servery, zálohování, archivace),
- rozšiřitelnost,
- sdílení systémových zdrojů,
- virtualizační platfoma Microsoft Hyper-V.

Požadavky na architekturu DDC jsou uvedeny v obr. č. 1

Součástí DDC musí být i další potřebné příslušenství nezbytné k řádnému zprovoznění Dodávky a jejímu optimálnímu provozu (mj. napájecí kabely, adaptéry, propojovací kabely mezi servery a LAN a SAN switchi, případně další nezbytné síťové i jiné komponenty).



Obrázek č. 1 – obecné schéma DDC

Název	Popis
Detašované pracoviště	Odloučené pracoviště zadavatele. Spojení s DDC bude zajištěno pomocí virtuálního privátního spojení.
dark fibre	Nenasvícený optický kabel
IP - VPN	Virtuální privátní spojení – šifrované spojení realizované prostřednictvím sítě internet.
SAN	Storage area network (zkratka SAN) je dedikovaná (oddělená od LAN, WAN, atd) datová síť, která slouží pro připojení externích zařízení k serverům (disková pole, páskové knihovny a jiná zálohovací zařízení.
Internet	Internet je celosvětový systém navzájem propojených počítačových sítí („síť sítí“), ve kterých mezi sebou počítače komunikují pomocí rodiny protokolů TCP/IP. Společným cílem všech lidí využívajících Internet je bezproblémová komunikace (výměna dat).
Fyzické servery virtualizační vrstvy	Fyzický hardware (servery) určený pro virtualizaci operačních systémů a služeb
Virtuální server – sdílené systémové zdroje	Virtuální server (VS) je server běžící na virtualizovaném hardware. VS běží na stejném fyzickém stroji jako jiné virtuální servery a je v mnoha ohledech funkčně ekvivalentní se samostatnými fyzickými počítači. Zdroje fyzického serveru jsou sdílené pro více virtuálních serverů.
Virtuální servery – dedikované systémové zdroje	Virtuální server (VS) je server běžící na virtualizovaném hardware. VS běží na stejném fyzickém stroji jako jiné virtuální servery a je v mnoha ohledech funkčně ekvivalentní se samostatnými fyzickými počítači. Zdroje fyzického serveru jsou alokované pro jednotlivé virtuální serverů. Nelze poskytnout více zdrojů, než má fyzický server k dispozici.
ÚLOŽIŠTĚ – datová pole	Zařízení pro centrální ukládání dat s vysokou dostupnosti. Zpravidla je k němu přistupováno z více serverů.
Archivace – páskové jednotky	Pásková jednotka (též označován jako streamer) je zařízení pro záznam dat, které provádí čtení a zápis dat na magnetickou pásku. Záznam na magnetické pásky se používá zejména pro archivaci a zálohování důležitých dat, typicky pro vytváření záloh obsahu pevných disků. Tento typ média je oblíbený pro jeho relativně nízkou cenu a dlouhou (ověřenou) životnost.
Zálohovací servery D2D	Zálohování dat na specializované diskové jednotky, určené pro zálohy u kterých je požadován vysoký výkon na vlastní provedení zálohy a rychlá obnova.

Tabulka č. 1 – popis obecného schéma DDC

3.1.1 Požadavky na licenční zajištění

Zadavatel dá k dispozici licence na produkty od společnosti Microsoft, které budou zapotřebí k implementaci požadovaných funkcionalit (vyjma licence na produkt Microsoft pro dohledový/monitorovací systém).

Současně Uchazeč v nabídce uvede seznam všech licencí včetně jejich počtu, které využije při návrhu architektury DDC.

3.1.2 Požadavky na hardware a software

Uchazečem navržená sestava HW nemusí detailně odpovídat navrženému uspořádání (obrázek č. 2a,b, obrázek č.3), avšak funkcionalita naznačených prvků jako i funkčnost celé sestavy musí minimálně splňovat anebo převyšovat funkcionalitu zde požadovaných prvků a také funkčnost Dodávky jako celku.

Rozsah a požadované vlastnosti kladené na všechny vyjmenované prvky sestavy předmětu plnění musí splňovat parametry uvedené v dalších kapitolách této přílohy zadávací dokumentace.

Uchazeč je povinen ve své nabídce uvést detailní technickou specifikaci jednotlivých nabízených sestav (HW i SW), které hodlá použít. U těch parametrů, které jsou požadované, musí uchazeč explicitně uvést, jak je naplňuje.

Zadavatel dále požaduje, aby Uchazeč uvedl ve své nabídce mimo ostatních požadavků uvedených v této zadávací dokumentaci také následující informace:

- rozměry a hmotnost každého relevantního prvku,
- nároky na napájení každého relevantního prvku,
- přehled všech typů podporovaných rozhraní (např. SAN, LAN, periferie),
- návrh rozmístění všech prvků v rámci datových rozvaděču a to v minimálním rozsahu, jaký je uveden v obrázku č. 2a,b.

3.1.3 Požadavky na záruční lhůty a dostupnost náhradních dílů

Zadavatel požaduje, aby každé použité zařízení (tj. veškerý dodaný HW a SW DDC) bylo pokryto (maintenance / carepack / záruka) od výrobce daného zařízení nebo software, a to v minimální délce 4 let s garantovanou dobou zprovoznění (uvedení do bezvadného stavu) v režimu potřebném pro splnění požadovaných SLA.(on-site). Jako minimální možný režim požadované záruky Zadavatel stanovil režim NBD – on site.

Zadavatel požaduje, aby součástí Dodávky byla pouze zařízení, u nichž je zajištěna dostupnost podpory výrobce pro každý použitý typ zařízení, a to v minimální stanovené době 6 let po uvedení zařízení do provozu.

3.1.4 Požadavky na energetickou úspornost

Uchazečem navržené položky v sestavě HW musí být klasifikovány jako energeticky úsporná.

Servery musí umožňovat dynamickou regulaci napětí, frekvence procesoru v závislosti na aktuálním zatížení daného serveru. Cílem je snížení nároku na spotřebu elektrické energie a následného chlazení Datového centra.

3.1.5 Požadavky na kompatibilitu

Pokud se uchazeč rozhodne pro dodávku HW a SW jiného výrobce se srovnatelnou funkcionalitou a stejnými nebo vyššími výkonnostními parametry než jsou požadované, musí být veškeré dodané hardwarové i softwarové komponenty řešení vzájemně kompatibilní.

V případě, že v průběhu implementace zjistí zadavatel nekompatibilitu, jdou veškeré takto vzniklé náklady k tíži uchazeče.

3.2 Umístění Datových center

Místem plnění předmětu veřejné zakázky je Datové centrum A umístěné v prostorách Zadavatele (Sokolovská ul.) a Datové centrum B je umístěno v lokalitě hl.m. Praha.

Propojení mezi datovými centry bude za pomocí 2 párů nenasvícených optických vláken, zajištěných Zadavatelem do úrovně pasivních prvků. Uchazeč tyto vlákna musí opatřit potřebnými aktivními prvky.

V každém datovém centru je k dispozici místo pro 10 standardizovaných uzamykatelných datových rozvaděčů šíře 600mm (případně maximálně 2 datové rozvaděče mohou být i šíře až 800mm).

Popis parametru	Minimální podpora parametru
Klasifikace prostředí	Tier II +zařízení redundantně napájena
Redundance všech kritických systémů	(UPS-baterie n + 1, motorgenerátor, distribuce napětí, chlazení) zajišťující částečnou servisovatelnost za provozu.
Dostupnost NDC	není sledováno
Chlazení	studená ulička částečně; existují tepelné mosty
Konektivita	DWDM - 2 páry černé vlákno 2 páry nenasvícených optických vláken
Požární bezpečnost	elektrická požární signalizace,
Fyzická bezpečnost	strážní služba 24 × 7
	systém kontroly vstupu pomocí elektronických identifikačních karet, el. samozamykací zámek Abloy
	IP kamery s detekcí pohybu
	IP kamery s detekcí pohybu
	Záznam cca 72 hodin
Systém zdvojené podlahy	Dimenzovaná na vysokou nosnost a zátěž,
	antistatická.
Napájení a záloha	Vlastní transformátorová stanice - vlastník/správce objektu ČSSZ,
	dvě nezávislé VN připojení,
	UPS - baterie n + 1, motorgenerátor zabezpečující nepřetržité napájení,
	Třífázové 32A/ jednofázové 16A rozvody do datového sálu pod podlahou
Palivové hospodářství	vlastník/správce objektu ČSSZ
Monitoring non IT technologií	částečně

3.3 Požadavky na Datové centrum A nebo Datové centrum B

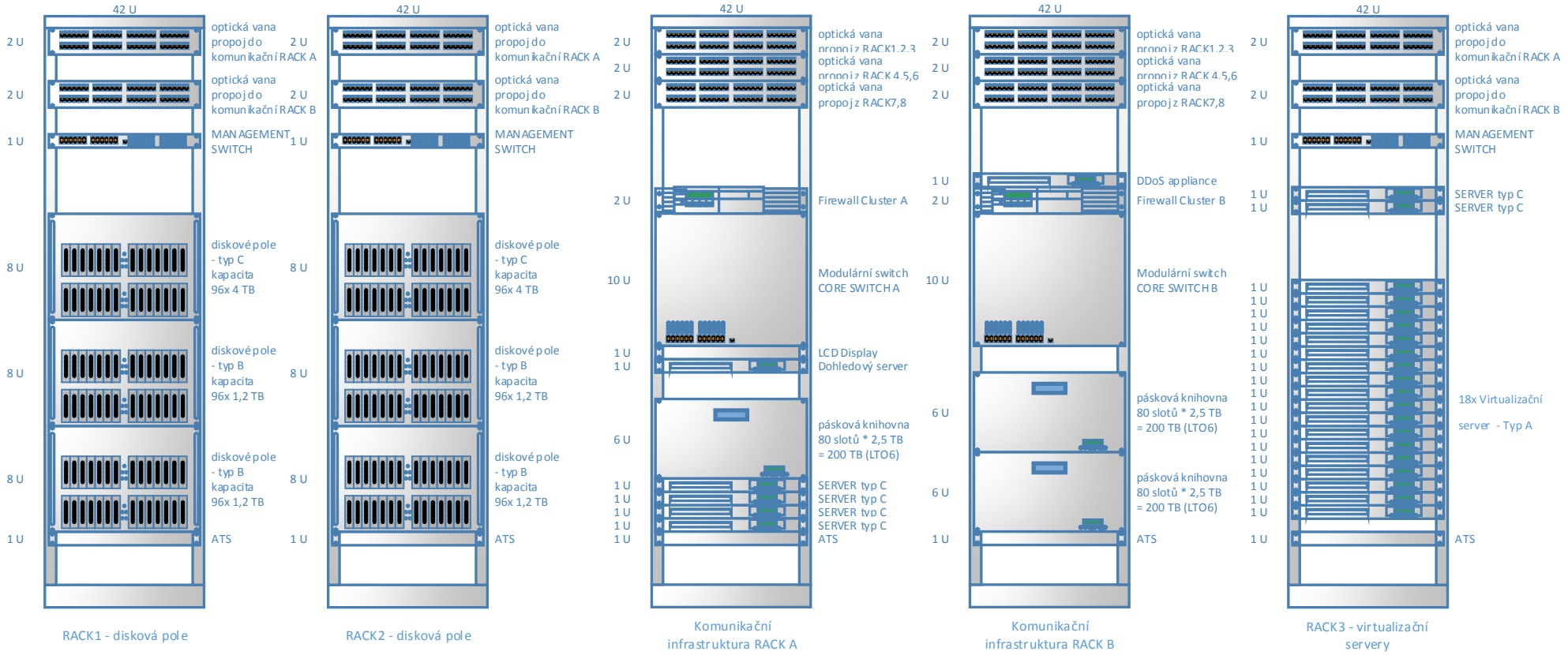
Každé Datové centrum A i Datové centrum B bude tvořeno maximálně 10 kusy RACK rozvaděčů s min. výškou 42U / šíře 600mm (případně maximálně 2 datové rozvaděče mohou být i šíře až 800mm). . V datových rozvaděčích bude nainstalováno veškeré vybavení (servery, switche, disková pole, routery apod.) potřebné pro bezproblémový provoz.

Propojení jednotlivých datových rozvaděčů bude realizováno optickými vlákny se zakončením v rámci optické vany každého datového rozvaděče. Páteřními prvky Datových center budou 2 modulární switche nebo soubor switchů a centrálně spravovaný firewall provozovaný v režimu clusteru.

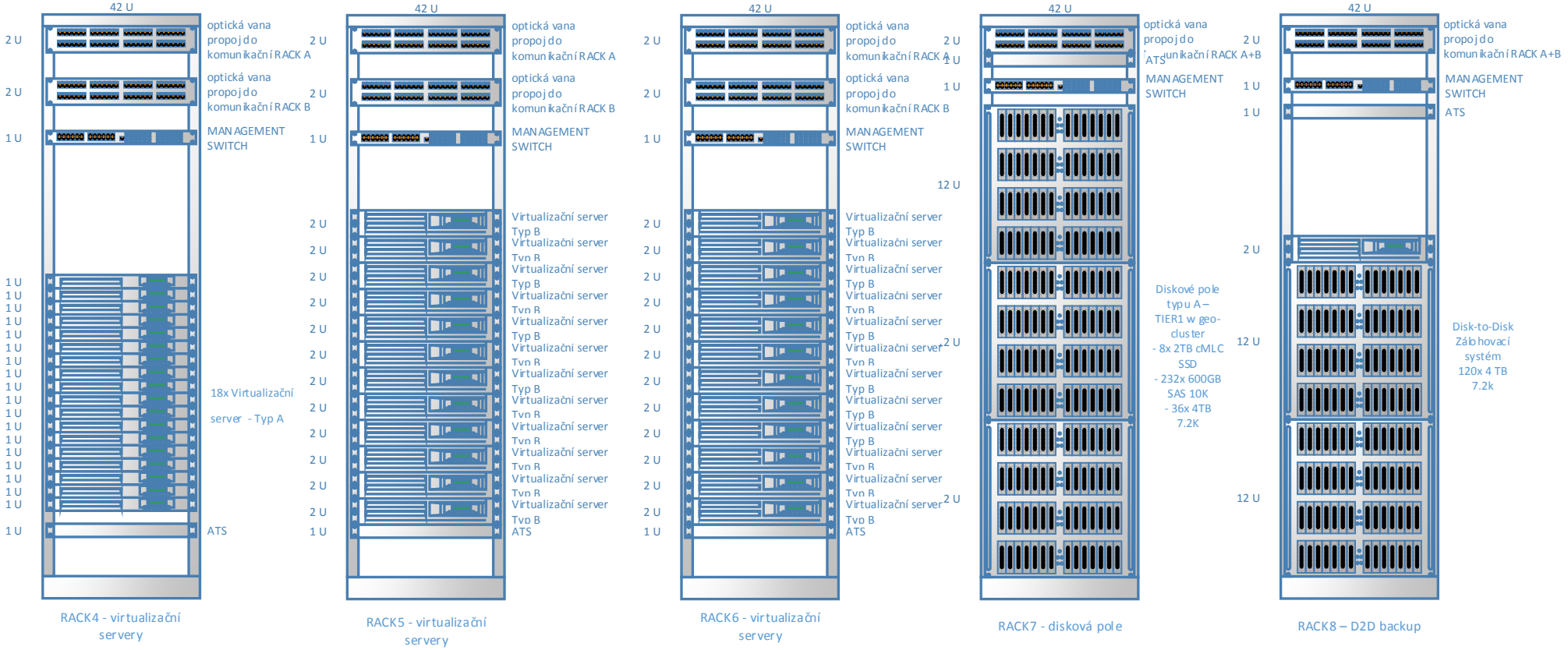
Datové centrum A i Datové centrum B bude obsahovat několik diskových polí různých výkonnostních charakteristik a podporovaných funkcionalit.

Virtualizační servery budou 2 a 4 soketové, vždy s napojením na disková pole. Součástí Datového centra bude také několik samostatných serverů mající lokální diskovou kapacitu pro služby, které nemohou být virtualizovány nebo jejich dostupnost má být zcela nezávislá na virtualizační platformě Microsoft Hyper-V. Vzorové schéma jednoho Datového centra A / Datového centra B je znázorněno na obrázku č. 2a,b.

Pro vyloučení všech pochybností Zadavatel uvádí, že DDC tedy i včetně všech použitých zařízení a prvků musí být v Datovém centru A i v Datovém centru B naprosto totožné. Zadavatel také zdůrazňuje, že tento bod popisuje vždy jen jedno ze dvou požadovaných totožných Datových center, a to včetně počtu kusů jednotlivých zařízení jen jednoho Datového centra A i Datového centra B. Pokud je uvedeno Datové centrum, rozumí se tím Datové centrum A nebo Datové centrum B.



Obrázek č. 2a –vzorové schéma Datového centra



Obrázek č. 2b –vzorové schéma Datového centra

3.3.1 Požadavky na komunikační infrastrukturu

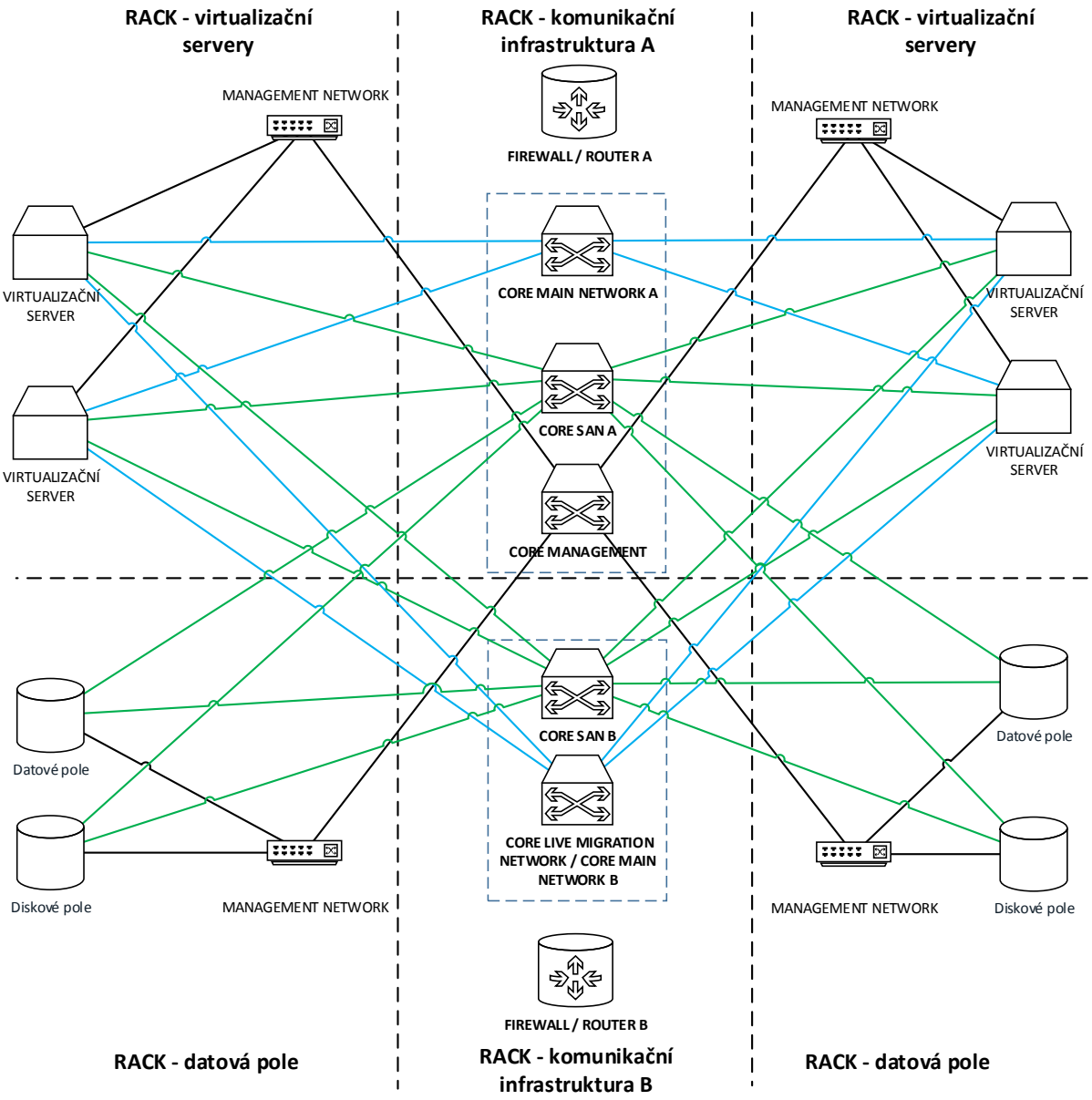
Komunikační infrastruktura Datového centra bude založená na bázi hvězdicové topologie. Centrálním uzlem budou 2 modulární switche (nebo soubor switchů) pracující v redundantním režimu.

Komunikační infrastruktura bude zajišťovat redundantní spojení mezi jednotlivými částmi (servery, diskové pole apod.) Datových center.

Přístup do Datových center bude zajištovat firewall provozovaný v režimu clusteru. Firewall bude zprostředkovávat site-to-site VPN spojení s ostatními datovými centry Zadavatele (např. Poříční právo, apod.) a detašovanými pracovišti Zadavatele. Též bude zajištovat VPN spojení typu klient-server pro mobilní uživatele.

Komunikační vrstva bude dále rozčleněna do potřebných VLAN skupin pro zajištění bezpečného provozu.

Schéma komunikační infrastruktury je zobrazeno na obrázku č. 3.



Obrázek č. 3 – komunikační schéma Datového centra

3.3.1.1 SAN

Storage area network (SAN) bude založena na technologii Fibre Channel (FC) s kapacitou 16 Gbps / port. Pro komunikaci je využito optických vláken.

SAN musí být provozována v režimu vysoké dostupnosti. Tomuto požadavku musí odpovídat zapojení všech prvků (diskové pole, servery, switche) a také patřičné nastavení softwarové části infrastruktury a prvků.

Virtualizační servery budou komunikovat s diskovými poli za použití metody „round robin“ pro zajištění vysoké dostupnosti a rozložení zátěže (obrázek č. 6)

Centrálními uzly komunikační infrastruktury SAN jsou modulární switche uvedené v bodě 3.3.1.8.

3.3.1.2 MAIN NETWORK

Main network je hlavní část komunikační infrastruktury. Probíhá zde veškerá TCP/IP komunikace. Datový provoz je oddělen do jednotlivých VLAN.

Síť je založena na technologii ethernet s kapacitou 10 Gbps / port. Spojení je realizováno za pomocí optických vláken. Virtualizační servery budou do této části sítě zapojeny redundantním způsobem, pro zajištění vysoké dostupnosti.

Hraničním prvkem datového centra je firewall pracující v režimu clusteru – viz bod 3.3.1.6.

Centrálními uzly této části komunikační architektury jsou modulární switche uvedené v bodě 3.3.1.8.

3.3.1.3 MANAGEMENT NETWORK

Management network je část komunikační infrastruktury určená pro monitorovací a jiné podpůrné služby (například pro připojení vzdálených managementů jednotlivých diskových polí a serverů).

Komunikace probíhá na základě TCP/IP protokolu s šířkou pásma do 1 Gbps / port. V každém datovém rozvaděči (vyjma komunikačních rozvaděčů A,B) je umístěn jeden řiditelný switch s potřebným počtem portů. Cílem switche je agregovat metalickou kabeláž v rámci datového rozvaděče. Propojení s centrálním modulárním switchem bude realizováno za pomocí optického vlákna.

Tato část infrastruktury má podpůrný charakter z provozoního hlediska. Proto nemusí být řešena redundantním způsobem.

Požadavky na aktivní prvky pro tuto část komunikační infrastruktury jsou uvedeny v tabulce č. 4.

3.3.1.4 Požadavek na propojení Datových center

Zadavatel požaduje propojit Datová centra nenasvícenými optickými vlákny. K dispozici jsou 2 vlákna, jedno pro technologii FC, druhé pro TCP/IP.

Požadovaná minimální kapacita spoje typu Fibre Channel (FC) je 8 Gbps. Požadovaná minimální kapacita spoje typu TCP/IP je 10 Gbps.

Předpokládaná délka optických kabelů je do 30 km.

Propojení TCP/IP mezi datovými centry bude zálohován VPN spojením prostřednictvím sítě Internet.

3.3.1.5 Požadavek na propojení datových rozvaděčů v rámci Datového centra

V rámci Datového centra budou datové rozvadeče propojeny za pomocí optických vláken.

Zadavatel nechá na uvážení Uchazeče, zda pro realizaci použije vícevláknové optické kabely nebo svazky z jednovláken v chráničce. V obou případech kabeláž vedená mimo datový rozvadeč musí být zakončena v optické vaně s řádným popisem.

Kabeláž uvnitř datových rozvaděčů bude realizována za pomocí optických a metalických patch kabelů potřebných délek. Propoje musí být realizovány takovým způsobem, aby se plně vyhovělo požadavku na redundanci provozu.

3.3.1.6 Požadavky na firewall

Firewallový cluster musí podporovat protokol IPv4 a IPv6. Řešení nesmí být žádným způsobem licencováno na počet klientů/uživatelů/stanic/serverů (apod.) nebo použitá licence nesmí tento počet nijak limitovat.

Firewallový cluster musí podporovat připojení s šířkou pásma 2x10Gbit.

Firewall musí podporovat inspekci paketů IPS a inspekci aplikačním firewallem na L3. Dále musí být rozšířený o kontrolu AntiSpam a WebContentFilter a nastaven takovým způsobem, aby zabraňoval šíření škodlivého software v rámci komunikační infrastruktury.

Minimální technické požadavky:

- minimální počet současných připojení - 7.000.000,
- minimální počet nových připojení/s - 180.000,
- IPv6 ready,
- celková propustnost firewallu - 20Gbps,
- zajištění vysoké dostupnosti funkcí cluster,
- nezávislost výkonu firewallu na velikosti paketu,
- podpora režimu vysoké dostupnosti v režimech A-P i A-A (navržené řešení musí umožňovat přepnutí z režimu A-P do režimu A-A bez změn v licencování),
- podpora dynamickych routovacích protokolů,
- nastavování pravidel na úrovni koncových portů (fyzických, virtuálních – integrace do MS Hyper-V),
- licencování nezávislé na počtu uživatelů, chráněných IP adres,
- minimální počet souběžných IP Sec tunelů – 1000ks,
- minimální počet uzlů clusteru: 2.

Minimální technické požadavky na VPN spojení:

- VPN nesmí být licencována na počet současně připojených klientů,
- možnost rozšíření na ověřování pomocí tokenů s časovým kódem,
- ověřování klientů VPN v rámci Active Directory,
- šifrování VPN tunelu AES/SHA2 256bit,
- IPv6 ready,
- celková propustnost VPN na FW - 8Gbps,
- minimální počet VPN uživatelů - 1000.

Minimální technické požadavky na firewall cluster parametry:	
Network Interfaces	4 x 10GbE SFP+
	8 x 10/100/1000 RJ45
Antivirus Throughput (Flow)	2 Gbps

Firewall Max Concurrent Session	7000000
Firewall New Sessions per second	180000
Firewall Throughput 1518 Bytes	20 Gbps
Firewall Throughput 512 Bytes	20 Gbps
Firewall Throughput 64 Bytes	20 Gbps
IPS Throughput (HTTP)	2.0 Gbps
Antivirus Throughput (Proxy)	1.5 Gbps
IPSec Throughput - 512 Byte Packet	8 Gbps

Tabulka č. 2 – požadavky na firewallovový cluster

Zadavatel nestanovuje podmínky, zda-li řešení firewallu má být provozováno na fyzickém hardware výrobce firewallu nebo formou virtualizace. V případě volby virtualizace je uchazeč povinen v nabídce k ceně softwarového řešení započítat hardware nutný pro provoz virtuálních appliance s požadovaným výkonem.

Řešení firewallů musí být navrženo takovým způsobem, aby v obou Datových centrech byly firewally centrálně spravovány v rámci jednotného mamagementu, který umožnuje správu fyzické i virtuální sítě (integrace do virtualizační platformy Microsoft Hyper-V).

Jednotlivé uzly (nody) firewalového clusteru musí být umístěné v různých datových rozvaděčích v rámci Datového centra, z důvodu zajištění vysoké dostupnosti i při selhání datového rozvaděče (např. eliminace lidské chyby při údržbě prvků v rozvaděči).

3.3.1.7 Požadavky na odolnost proti DDoS útokům

Datové centrum musí být vybaveno hardwarově akcelerovaným zařízením umožňující včasnou detekci DDoS útoků na úrovni komunikační vrstvy L3 a L4 a umožnůjící zmírnění důsledků DDoS útoků.

Požadavky na zařízení:

- umístitelnost do datového rozvaděče (výška max. 2U),
- celková propustnost 1 Gbps,
- minimální počet současných spojení - 1.000.000,
- inspekce packetů (Heuretistická analýza, monitorování),
- dynamická reputace IP adres (analýza) vč. aktualizací dat od výrobce,
- reportování (email, snmp).

3.3.1.8 Požadavky na centrální modulární switche

Datové centrum bude vybaveno dvěma modulárními switchy (nebo souborem switchů zajišťující totožnou funkcionalitu).

Switche budou uložený ve dvou různých datových rozvaděčích a nakonfigurovány takovým způsobem, aby v případě výpadku jednoho centrálního switche nebo celého datového rozvaděče s komunikační infrastrukturou, druhý switch zachoval funkcionalitu datového centra a jim poskytovaných služeb.

Zadavatel nepředepisuje, zda centrální switche mají být modulární, nebo nabídne soubor switchů s centrálním managementem. V případě použití souboru switchů, musí být propoje mezi switchi realizovány s dodatečně dimenzovanou kapacitou.

Požadované parametry jednoho modulárního switche (nebo souboru switchů)

Číslo	Vlastnost/komponenta	Požadované minimální parametry
1.	Switch s managementem	ANO
2.	Jednotný management pro více switchů	ANO – vč. podpory integrace Hyper-V prostředí
3.	Napájecí zdroj	Redundantní
4.	Souhrná přepínací kapacita	500 Gbps
5.	Provedení	RACK - velikost do 12U (nebo taková velikost, aby switch byl umístitelný v rámci komunikačního RACKu)
6.	Podporované protokoly	IEEE 802.1q, IEEE 802.1s, IEEE802.3ad, IEEE 802.3az, IEEE802.1AB SNMP v1/v2c/v3, IEEE 802.1p, IEEE 802.1P, IEEE 802.3ae, OSFP, IPv4/IPv6 routing, BGP
7.	IPv6 ready	ANO (Dual-Stack IPv4/IPv6)
8.	Podpora funkcionalit vrstev L2/L3	bez omezení
9.	Nativní podpora Fiber Channel	ANO (vč. FCoE)
10.	Podporované typy portů	Fibre Channel – 16 gbps Ethernet – 0.1/1/10 gbps
11.	Počet portů Fiber Channel	Nutný počet pro zapojení všech prvků datového centra + 10% rezerva
12.	Počet portů Ethernet	Nutný počet pro zapojení všech prvků datového centra + 10% rezerva
13.	Software a licence	K zařízení musí být dodán veškerý potřebný software a licence, umožňující požadované funkcionality.

Tabulka č. 3 – minimální požadavky na centrální switche

3.3.1.9 Požadavky na switche pro podpůrnou část komunikační architektury – MANAGEMENT NETWORK

Zadavatel požaduje dodání 8 kusů switchů v minimální konfiguraci dle tabulky č. 4:

Číslo	Vlastnost/komponenta	Požadované minimální parametry
1.	Switch s managementem	ANO
2.	Počet portů	24
3.	PoE	Není vyžadováno
4.	Typ portů	2x SPF 1000 mbps, 22x RJ45 10/100/1000 mbps
5.	Provedení	RACK - velikost do 1U
6.	Přepínací kapacita	10 gbps
7.	Podporované protokoly	IEEE 802.1Q, IEEE 802.1S, IEEE802.3ad, IEEE 802.3az, IEEE802.1AB SNMP v1/v2c/v3

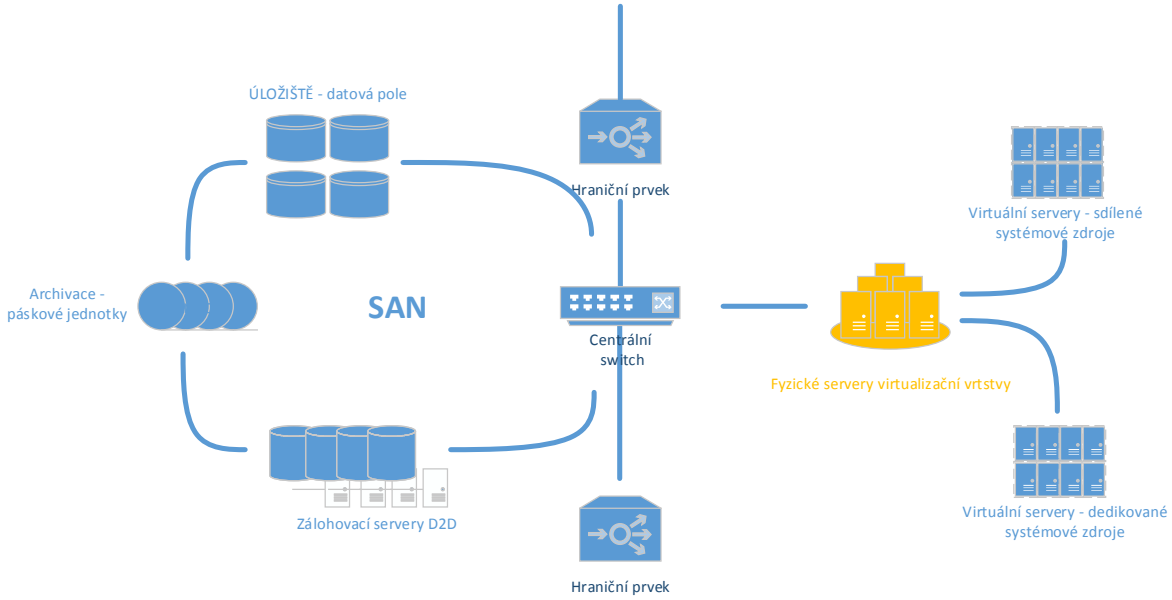
Číslo	Vlastnost/komponenta	Požadované minimální parametry
8.	Vzdálená správa s centralizovaným management	ANO
9.	Podpora velkých (JUMBO) paketů	ANO
10.	IPv6 ready	ANO (Dual-Stack IPv4/IPv6)

Tabulka č. 4 – minimální požadavky na switche pro MANAGEMENT NETWORK

3.3.2 Požadavky na fyzické servery virtualizační vrstvy

Zadavatel požaduje dodání fyzických serverů umožňující provozování virtualizační platformy Microsoft Hyper-V v poslední uvolněné verzi.

Servery musí být dodané v konfiguracích splňující minimální parametry uvedené v tabulce č.5 a tabulce č.6. Značku a typ serverů může zvolit dodavatel, avšak vždy musí být dodána modelová řada poslední výrobcem uvolněné modelové generace. Rozhodným datem pro určení modelové generace serveru je poslední den konce lhůty pro podání nabídek.



Obrázek č. 4

Zadavatel požaduje dodání serverů pro Datové centrum:

- s požadovanými minimálními parametry uvedenými v Tabulce č. 5 v počtu 36 kusů (TYP A),
- s požadovanými minimálními parametry uvedenými v Tabulce č. 6 v počtu 24 kusů (TYP B)

od jednoho uchazečem vybraného výrobce. V rámci jedné specifikace nelze dodat servery různých typů, byť by splňovali minimální stanovené parametry.

Číslo	Vlastnost/komponenta	Požadované minimální parametry
1.	Počet CPU	2
2.	Počet fyzických jader	min. 14 na CPU
3.	Počet souběžně zpracovaných vláken (celkově)	min. 28 na CPU
4.	Základní frekvence procesoru	2.6 GHz
5.	Provedení	RACK - velikost do 1U
6.	Napájení	redundantní napájecí zdroje (min. 2)
7.	Rodina procesoru	x-86 (podpora 64bit), podpora virtualizace
8.	Diskový subsystém	kapacita 100 GB v režimu RAID 1
9.	RAM	384GB
10.	SAN HBA	2x16Gb (2x single-port HBA)
11.	LAN	4x 10Gb
12.	Plně 64bit HW a SW architektura	požadováno
13.	Hardwarová akcelerace šifrování AES	požadováno
14.	Vzdálený management	KVM, console, virtual media

Tabulka č. 5 – minimální parametry virtualizačního serveru – TYP A

Číslo	Vlastnost/komponenta	Požadované minimální parametry
1.	Počet CPU	4
2.	Počet fyzických jader	min. 12 na CPU
3.	Počet souběžně zpracovaných vláken (celkově)	min. 24 na CPU
4.	Základní frekvence procesoru	2.4 GHz
5.	Provedení	RACK - velikost do 2U
6.	Napájení	redundantní napájecí zdroje (min. 2)
7.	Rodina procesoru	x-86 (podpora 64bit), podpora virtualizace
8.	Diskový subsystém	kapacita 100 GB v režimu RAID 1
9.	RAM	768GB
10.	SAN HBA	2x16Gb (2x single-port HBA)

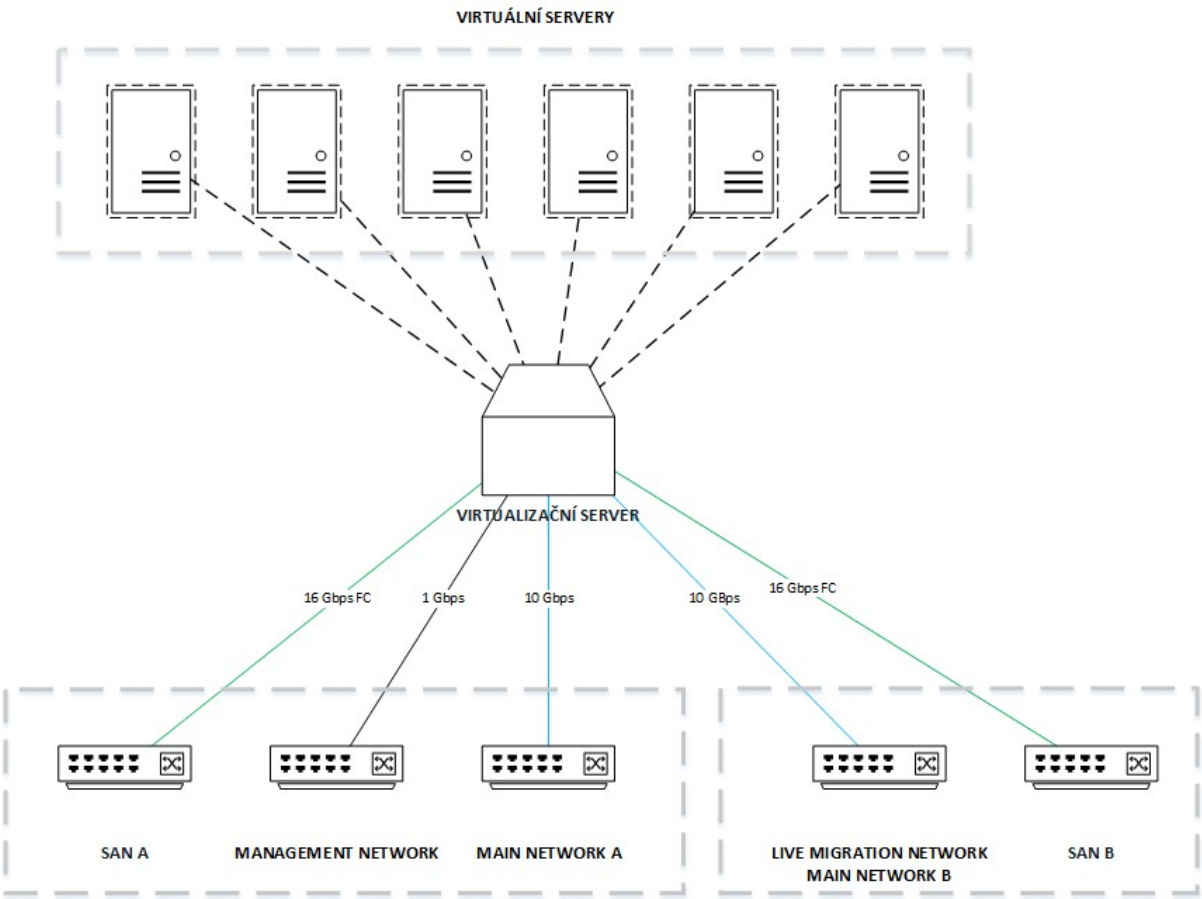
Číslo	Vlastnost/komponenta	Požadované minimální parametry
11.	LAN	4x 10Gb
12.	Plně 64bit HW a SW architektura	požadováno
13.	Hardwarová akcelerace šifrování AES	požadováno
14.	Vzdálený management	KVM, console, virtual media

Tabulka č. 6 – minimální parametry virtualizačního serveru – TYP B

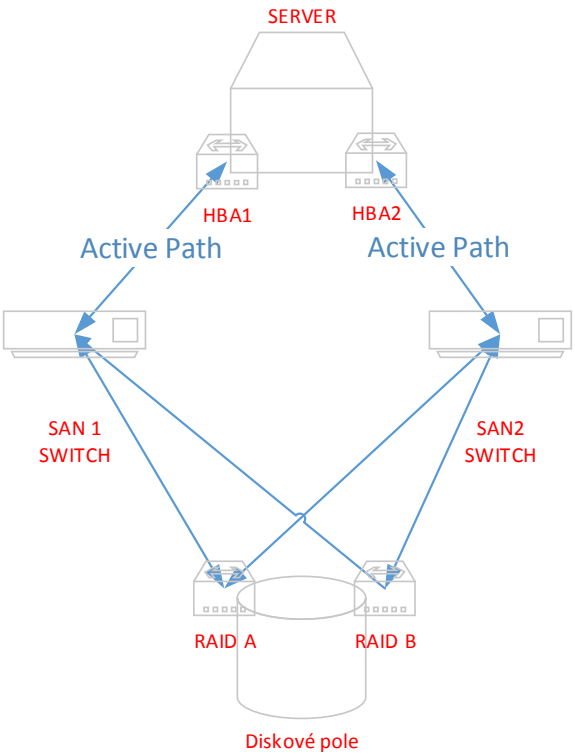
3.3.2.1 Požadavky na zapojení do komunikační infrastruktury

Každý fyzický server musí být připojen do komunikační infrastruktury redundantním způsobem. Popis komunikační infrastruktury je uveden v bodě 3.3.1. Minimální požadavky jsou uvedeny na obrázku číslo 5. – zapojení jednotlivého virtualizačního serveru do komunikační infrastruktury, a lze je charakteritizovat takto:

- spojení s diskovými poli SAN redundantním způsobem (trasa A, trasa B) o kapacitě jedné trasy 16 Gbps v řežimu Active-Active (obrázek č. 6),
- spojení s hlavní sítí (MAIN NETWORK) redundantním způsobem (trasa A, trasa B) o kapacitě jedné trasy 10 Gbps,
- spojení se síti pro správu (MANAGEMENT NETWORK) o minimální šířce pásma 1 Gbps,
- spojení se sítí pro přenos virtuálních serverů za provozu (LIVE MIGRATION NETWORK) o kapacitě 10 Gbps, která však může (ale nemusí) být sdílena s hlavní sítí (MAIN NETWORK).



Obrázek č. 5 – zapojení jednotlivého virtualizačního serveru do komunikační infrastruktury



Obrázek č. 6 – zapojení virtualizačního serveru do SAN části komunikační infrastruktury v režimu Active-Active

3.3.2.2 Požadavky na kompatibilitu

Uchazečem navržené servery musí být zcela kompatibilní s ostatními částmi DDC (softwarová i hardwarová část).

Uchazečem navržené virtualizační servery (Tabulka č. 5, tabulka č. 6) musí být navzájem kompatibilní do té míry, aby podporovali veškeré funkcionality, které jim umožňuje virtualizační platforma Microsoft Hyper-V. Zejména se jedná o živé migrace virtuálních serverů napříč virtualizačními servery.

3.3.3 Požadavky na samostatné servery s vlastním diskovým prostorem (TYP C)

V Datovém centru bude umístěno minimálně 6 samostatných serverů mající vlastní diskový prostor. Zadavatel přepokládá využití serverů v následujících oblastech:

- provoz systémů a aplikací, které nemohou být z technických nebo jiných důvodů virtualizovány,
- provoz systémů a aplikací, u kterých je nutno zajistit nezávislost na virtualizační platformě datového centra – například dohledový a monitorovací systém datového centra,
- provoz software pro zálohování a archivaci.

Minimální technické požadavky na jeden server jsou vedeny v tabulce č. 7

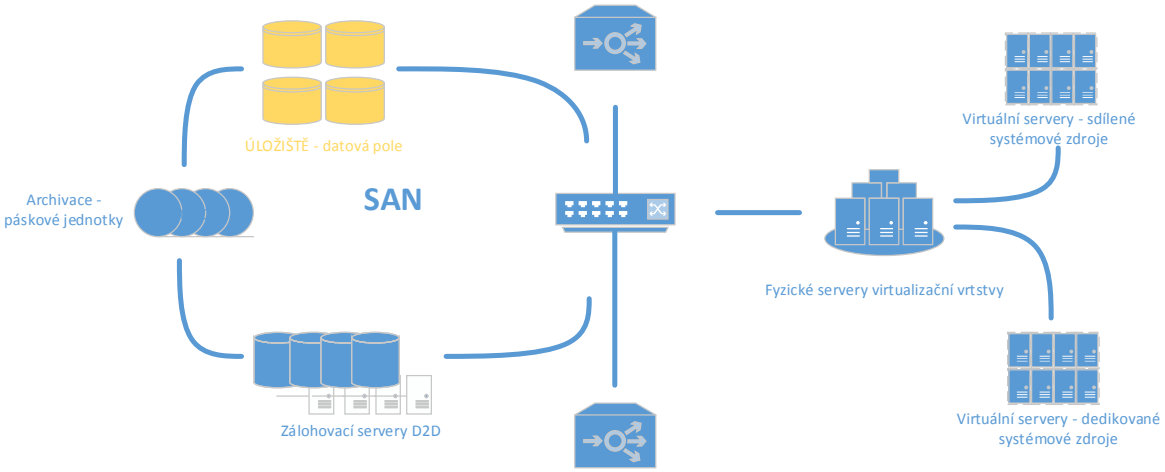
Číslo	Vlastnost/komponenta	Požadované minimální parametry
1.	Počet CPU	1
2.	Výkon jednoho procesoru (body dle výkonnostního indexu www.passmark.com)	14 000
3.	Provedení	RACK - velikost do 1U
4.	Napájení	redundantní napájecí zdroje (min. 2)
5.	Rodina procesoru	x-86 (podpora 64bit)
6.	Počet pevných disků	8
7.	Kapacita a typ pevného disku	600 GB SAS 10K
8.	RAM	96 GB
9.	SAN HBA	2x16Gb (2x single-port HBA)
10.	LAN	4x 10Gb
11.	Plně 64bit HW a SW architektura	požadováno
12.	Hardwarová akcelerace šifrování AES	požadováno
13.	Vzdálený management	KVM, console, virtual media

Tabulka č. 7 – minimální parametry serveru s vlastním diskovým prostorem– TYP C

3.3.4 Požadavky na disková pole

Disková pole slouží v rámci Datového centra jako centrální úložiště dat. V Datových centrech budou provozovány systémy s různou náročností na výkon diskového subsystému, zadavatel požaduje dodání více diskových polí s různou výkonnostní charakteristikou.

V případě hostování systémů, které musí z licenčních důvodů být provozovány na fyzicky odděleném clusteru, je nutno mít k dispozici více než jedno diskové pole v rámci jednoho Datového centra.



Obrázek č. 7 – datová úložiště

Komunikace diskových polí s virtualizačními servery zajišťuje komunikační architektura SAN specifikovaná v bodě 3.3.1.1.

Členění diskových polí

- **Diskové pole TYP A** – diskové pole pro střední a velké podniky – třída enterprise. Minimálně 250 diskových jednotek (HDD/SSD). Zajišťuje konstantně vysoký výkon při využití všech pokrokových služeb (akcelerace diskových svazků za pomocí SSD, vícenásobný počet dedikovaných kontrolerů pro přístup k datům nebo souborovým systémům, funkce geografický cluster, tenká provize diskových svazků, sníkování, podpora MPFS, pNFS, apod.) Vysoký stupeň redundance a odolnosti proti výpadku (kontrolery, napájecí zdroje). Počet připojitelných hostů min. 512.
- **Diskové pole TYP B –** diskové pole pro malé a střední podniky – třída entry. Maximálně 150 diskových jednotek HDD. Diskové pole sestaveno výhradně z výkonných disků SAS 10K. 2 kontrolery zajišťují redundantní přístup k datům. Pole má redundantní napájecí zdroje. Diskové pole poskytuje škálu základních funkcí a asynchronní replikaci dat mezi diskovými poli. Počet připojitelných hostů min. 64.
- **Diskové pole TYP C -** diskové pole pro malé a střední podniky – třída entry. Maximálně 150 diskových jednotek HDD. Diskové pole sestaveno výhradně

z vysokokapacitních disků (min. 4TB/disk). 2 kontrolery zajišťují redundantní přístup k datům. Pole má redundantní napájecí zdroje. Diskové pole poskytuje škálu základních funkcí, replikace dat mezi diskovými poli není potřebná. Počet připojitelných hostů min.64.

V rámci datového centra budou nainstalovány tato disková pole:

TYP A – 1 kus (minimální parametry dle tabulky č. 8)
TYP B – 4 kusy (minimální parametry dle tabulky č. 9
TYP C – 2 kusy (minimální parametry dle tabulky č. 10

3.3.4.1 Minimální požadavky na diskové pole TYP A

Číslo řádku	Požadavek na funkcionalitu nebo parametr	Minimální požadavky
1.	Celkový počet kontroléru (jak pro přístup k datům, tak souborovým systémům)	4
2.	Minimální propustnost systému na backend portech SAS	6Gbps
3.	Dodržena architektura HA (tedy min. zdvojení klíčových komponent)	ANO
4.	Nativní Fibre Channel konektivita pole pro blokový přístup	8 x 16Gbps
5.	Počet portů 10Gb ethernet pro souborový přístup	2
6.	Možnost budoucího rozšíření FC konektivity pole pro blokový přístup bez přerušení produkce a výpadku systému	až 16x16Gbps
7.	Možnost budoucího rozšíření iSCSI konektivity pole pro blokový přístup bez přerušení produkce a výpadku systému	až 4x10Gps
8.	Možnost budoucího rozšíření FCoE konektivity pole pro blokový přístup bez přerušení produkce a výpadku systému	až 4 x10Gps
9.	Možnost budoucího rozšíření Ethernet konektivity pole pro souborový přístup bez přerušení produkce a výpadku systému	min 4x10Gps
10.	Minimální počet Fibre Channel portů použitelných pro replikace (online synchronizaci obsahu polí)	2
11.	Celková hrubá velikost TIER 0 (**SSD** disků) je minimálně 23TB. Minimální počet disků v tomto TIERu musí být 12ks (například 12 x 1.92 TB)	23 TB
12.	Celková hrubá velikost TIER 1 (SAS 2,5“ 10.000 rpm) je minimálně 200 TB. Minimální počet disků v tomto TIERu musí být 348ks (například 348 x 600 GB)	200 TB
13.	Celková hrubá velikost TIER 2 (NS-SAS disky 7200 rpm) je minimálně 210TB. Minimální počet disků v tomto TIERu musí být 54 (například 54x 4TB)	210 TB
14.	Upgrade komponent včetně upgrade firmware řadiče a dalších komponent nebo výměna vadných komponent musí být možná bez přerušení provozu	ANO
15.	Disky jednotlivých TIERů mají stejnou velikost	ANO
16.	Zálohovaná systémová cache každého z kontrolerů	min. 4 GB
17.	Zdvojená systémová cache zálohována pomocí UPS (nebo bateriemi či kondenzátory v řadičích)	ANO
18.	Možnost rozšíření na maximální počet disků	min 512
19.	Podpora synchronní i asynchronní replikace datového obsahu na další diskové pole tohoto typu, na úrovni programového vybavení pole	OBSAHUJE
20.	Licence software pro tvorbu lokálních a vzdálených replik (klonů a snapů) uložených dat a pro zajištění aplikační datové konzistence vytvořených replik pro neomezený počet aplikačních a souborových hostů. Funkcionalita a licence musí pokrývat stav, kdy jsou například data databázového systému Microsoft SQL rozprostřena na více LUN a vytvořením repliky je vytvořen obraz všech zainteresovaných LUN ke stejnému času.	OBSAHUJE
21.	Licence software pro synchronní replikaci blokové a souborové storage do vzdálené lokality se schopností vytvářet plnohodnotné klony, obnovení klonu (resynchronizace) nutná inkrementálním způsobem (tedy pouze modifikované bloky od poslední synchronizace), vytváření a management klonů plně v kompetenci diskového pole	OBSAHUJE

Číslo řádku	Požadavek na funkcionalitu nebo parametr	Minimální požadavky
22.	Licence software pro virtual/thin provisioning blokových i souborových systémů a jejich replik (lokální i vzdálené)	OBSAHUJE
23.	Licence software pro plně automatický tiering blokového úložiště (na základě systémových statistik nebo uživatelských nastavení) pro celou dodávanou kapacitu a pro všechny tři dodávané tiery (SSD, SAS, SATA)	OBSAHUJE
24.	Licence software pro využití SSD disků, které budou sloužit jako rozšířená Cache oblast úložiště	OBSAHUJE
25.	Velikost rozšířené flash Cache fungující jako nativní cache	min. 200 GB
26.	Licence software pro sledování zatížení jednotlivých oblastí diskového systému, jednotlivých aplikačních hostů a na nastavení QOS (quality of service)	OBSAHUJE
27.	SW musí automaticky zajistit konzistenci ukládaných dat, a to jak při ukládání, tak i zálohování a obnově dat	ANO
	Software musí dále umožňovat a splňovat a obsahovat:	
28.	Centrální správu celého pole z grafického rozhraní	ANO
29.	Licencováno na veškerou poptávanou fyzickou a logickou kapacitu, všechny poptávané porty a alespoň 512 připojených fyzických a virtualních serverů	ANO
30.	Podporu pro MPFS (multipath file serving) nebo pNFS (parallel network file system) pro aplikace vysoce náročné na výpočetní výkon	ANO
31.	Možno dvojcestné konektivity (na blokové úrovni včetně funkce load ballancing pro neomezený počet připojených serverů) pro běžně dostupné OS	ANO
32.	Podpora protokolu NDMP (Network Data Management Protocol)	ANO
33.	Přístup k datům je možný prostřednictvím protokolů NFS v3 a **v4**, CIFS	ANO
34.	Podpora deduplikace a komprese uložených dat (včetně replik LUN) je nativní součást řešení	ANO
35.	Integrace do prostředí platformy Microsoft Hyper-V 2012 R2	ANO
36.	Integrace s kompresí pro Windows CIFS jako nativní součást	ANO
37.	Podpora alespoň 10 TB souborových systémů	ANO
38.	Migrace a rozšiřování jednotlivých LUNů a Volumů bez výpadku systému a bez závažného dopadu na výkon systému	ANO
39.	Podporou RAID 1, 5, 6, 10 a možností kombinovat různé technologie (SAS, NL-SAS, SSD v rámci jednoho systému)	ANO
40.	Možnost online migrace LUN z jedné RAID skupiny (například RAID 5) na jinou RAID skupinu (RAID 1/RAID 10) v rámci diskového pole pod zátěží a bez výpadku	ANO
41.	Použití plnohodnotného LUN masking software s podporou maskování objektů 1:N, tedy možnost maskovat LUN vůči libovolnému serveru bez omezení	ANO
42.	Velikost LUN alespoň 10 TB	ANO
43.	SW musí podporovat minimálně následující platformy a software: o MS Windows 2012 a vyšší, o RedHat Linux EL 7, o Microsoft SQL 2012 a vyšší	ANO

Tabulka č. 8 – minimální parametry diskového pole TYP A

3.3.4.2 Minimální požadavky na diskové pole TYP B

Číslo	Vlastnost/komponenta	Minimální požadované parametry
1.	Hrubá kapacita pole	min. 100 TB
2.	Typ disku	10 000 rpm, Dual-Port SAS, SFF
3.	Velikost disku	1,2 TB
4.	Počet diskových jednotek	96
5.	Počet řadičů úložných zařízení (SAN HBA)	min. 2 (redundantní provoz)
6.	SAN HBA - specifikace	min. 4x FC ports / 16Gb min. 4GB cache
7.	Velikost	max. 8U pro celé diskové pole vč. přídavných diskových polic
8.	Počet napájecích zdrojů	min. 2 (redundantní provoz)
9.	Vzdálený mgmt	požadováno
10.	Příslušenství	SPF+ moduly v požadovaném množství a min. rychlosti 16 Gb
11.	Asynchronní replikace dat mezi diskovými poli	požadováno
12.	Zabezpečení dat proti selhání	podpora RAID 1, 5, 6, 10

Tabulka č. 9 – minimální požadavky na diskové pole TYP B

3.3.4.3 Minimální požadavky na diskové pole TYP C

Číslo	Vlastnost/komponenta	Minimální požadované parametry
1.	Hrubá kapacita pole	min. 350 TB
2.	Typ disku	7 200 rpm, LFF
3.	Velikost disku	4 TB
4.	Počet diskových jednotek	96

Číslo	Vlastnost/komponenta	Minimální požadované parametry
5.	Počet řadičů úložných zařízení (SAN HBA)	min. 2 (redundantní provoz)
6.	SAN HBA - specifikace	min. 4x FC ports / 16Gb min. 4GB cache
7.	Velikost	max. 16U pro celé diskové pole vč. přídavných diskových polic
8.	Počet napájecích zdrojů	min. 2 (redundantní provoz)
9.	Vzdálený mgmt	požadováno
10.	Zabezpečení dat proti selhání	podpora RAID 1, 5, 6, 10

Tabulka č. 10 – minimální požadavky na diskové pole TYP C

3.3.4.4 Požadavky na zapojení do komunikační infrastruktury

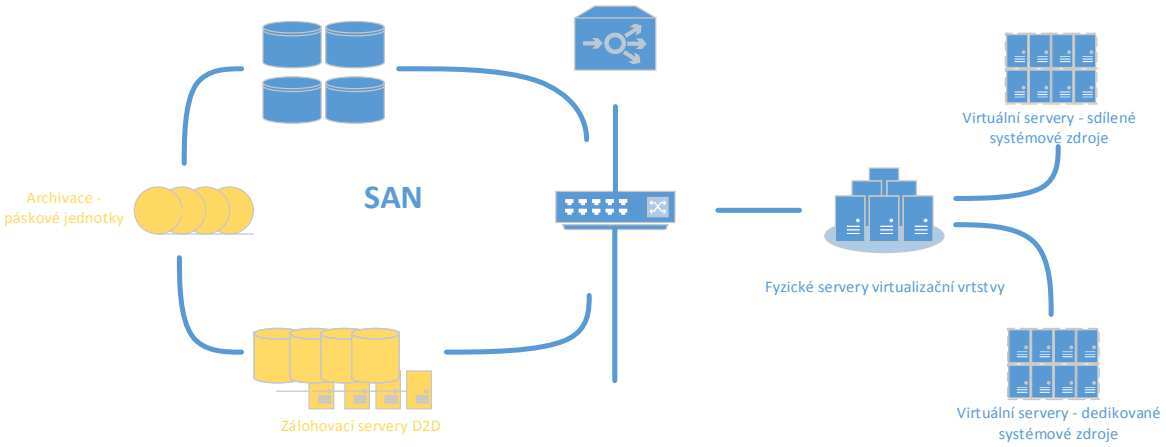
Disková pole musí být zapojena v rámci komunikační infrastruktury takovým způsobem, aby bylo vyhověno požadavkům zadavatele na vysokou dostupnost a přenosovou kapacitu. Každé diskové pole bude zapojeno přes minimálně 4 porty FC o rychlosti 16 Gbps a budou k dispozici 2 redundantní trasy. Schéma zapojení je znázorněno na obrázku č. 5.

3.3.4.5 Požadavky na hot-spare disky

Zadavatel požaduje, aby každé diskové pole bylo osazeno optimálním počtem hot spare disků, a to v souladu s doporučením výrobce datového pole vzhledem k jeho konfiguraci.

3.3.5 Zálohování a dlouhodobé ukládání dat

Součástí datového centra bude zálohovací (archivační) řešení. Primárním účelem je zajištění zálohy virtuálních serverů a na nich provozovaných aplikací a archivace dat pro delší časové období. Řešení musí být zcela kompatibilní s ostatními prvky Datového centra, zejména zvoleným hardware, virtualizační platformou a podporovanými operačními systémy a databázemi.



Obrázek č. 8 –zálohování a dlouhodobé ukládání dat

Zadavatel požaduje dodání diskového úložiště pro zálohy typu disk-to-disk a páskové knihovny pro zálohy typu disk-to-tape.

Archivace bude probíhat na totožném hardware, primárním archivačním úložištěm budou páskové knihovny.

Zadavatel nevyžaduje, aby pro zálohování a archivaci bylo použito unifikované (all-in-one) řešení od jednoho výrobce. Uchazeč může zvolit i řešení, které se skladá z částí (server, diskové pole, software) od různých výrobců (např. jiný dodavatel software a hardware). V každém případě je však nutno dodržet minimální funkční požadavky uvedené v bodě 3.3.5.1.

Zadavatel předpokládá, že pro provoz zálohovacího a archivačního řešení vyčlení maximálně 2 servery TYP C, specifikované v bodě 3.3.3 V případě, že řešení nabídnuté uchazečem bude vyžadovat vyšší výpočetní výkon, než jsou zadavatelem 2 vyčleněné servery schopny poskytnout, musí být dodatečný hardware součástí nabídky Uchazeče.

Kapacita pro zálohování bude tvořena:

- síťovým diskovým polem a aplikačním server nebo unifikovaným zařízením,
- páskovou knihovnou.

V případě nedostatečné kapacity zálohovacího řešení, bude možno alokovat část kapacity diskových polí typu C. Zálohovací řešení musí být tedy kompatibilní i s diskovým polem typu C.

3.3.5.1 Funkční požadavky na zálohovací řešení

Zadavatel zde specifikuje minimální požadavky na funkcionalitu zálohovacího řešení

Číslo	Vlastnost/komponenta	Požadované parametry
1.	Agentless backup - zálohování virtuálních strojů přímo z hypervizoru	ANO
2.	Zálohování agentem nainstalovaným uvnitř virtuálních strojů	ANO
3.	Zálohování metodou tvorby image - celé stroje, disky, svazky, oddíly	ANO

Číslo	Vlastnost/komponenta	Požadované parametry
4.	Zálohování datové - zvolené soubory a adresáře	ANO
5.	Vytváří plné, přírůstkové a rozdílové zálohy dle zvoleného plánu	ANO
6.	Komprese a šifrování záloh standardem AES 256 bit	ANO
7.	Možnost vyloučit nepotřebné soubory a adresáře z procesu zálohování	ANO
8.	Zálohování online - za plného provozu stroje, včetně otevřených souborů	ANO
9.	Zálohování offline - po nabootování stroje ze zaváděcího média (CD/DVD/USB)	ANO
10.	Možnost nastavit maximální možné vytížení sítě procesem zálohování	ANO
11.	Plánování zálohování na základě skupin a politik	ANO
12.	Možnost využít deduplikaci a zálohovat tak duplicitní data pouze jednou	ANO
13.	Wake On Lan - automatické probuzení uspaných strojů pro zálohování	ANO
14.	Možnost paralelního zálohování několika virtuálních strojů najednou	ANO
15.	Zálohování a migrace hostitelského stroje - offline ze zaváděcího média	ANO
16.	Zálohování MS Exchange	ANO – min. 8 serverů
17.	Zálohování MS SQL	ANO – min. 10 serverů
18.	Zálohování MS SharePoint	ANO – min. 8 serverů
19.	Zálohování MS Active Directory	ANO – min. 4 servery
20.	Zálohování operačních systému MS Windows, Linux	ANO – bez omezení
21.	Centralizovaná, vzdálená správa zálohování a obnovy	ANO
22.	Možnost lokální správy zálohování a obnovy - přímo na daném stroji	ANO
23.	Možnost vzdálené instalace agentů na zálohované stroje	ANO
24.	Možnost ovládání programu z příkazové řádky	ANO
25.	Poskytuje možnost skriptování	ANO
26.	Podrobné logování a reportování s možností zasílání na email	ANO
27.	Možnost připojit zálohu disku, svazku, oddílu jako virtuální jednotku	ANO
28.	Ukládání záloh do lokálních a síťových úložišť, NAS, FTP	ANO

Číslo	Vlastnost/komponenta	Požadované parametry
29.	Podporuje rozhraní S-ATA, SCSI, iSCSI, USB	ANO
30.	Ukládání záloh metodou Disk to Disk to Tape	ANO
31.	Možnost replikovat zálohy do několika úložišť	ANO
32.	Možnost postupného přesouvání záloh do jiného úložiště	ANO
33.	Automatická verifikace a konsolidace záloh	ANO

Tabulka č. 11 – požadavky na zálohovací řešení

Uchazečem nabídnutý zálohovací a archivační software musí umožňovat zálohu všech serverů (fyzických i virtuálních) provozovaných v rámci DDC. Zadavatel požaduje dodání zálohovacího a archivačního software, který nemá licenční omezení nebo je licenčně vázán na fyzický hardware.

Z hlediska specializovaných serverů, Zadavatel přepokládá, že v rámci datového centra bude provozováno:

- minimálně 10 Microsoft SQL serverů,
- minimálně 8 Microsoft Exchange serverů,
- minimálně 8 SharePoint serverů,
- minimálně 4 Active Directory serverů.

Uchazečem zvolený typ licence musí pokrýt minimálně tento počet specializovaných serverů a musí dále umožnovat zálohu fyzických nebo virtuálních serverů bez omezení jejich počtu.

3.3.5.2 Funkční požadavky na archivační řešení

Požadavky na achivaci dat jsou totožné s požadavky na zálohování. Primárním úložištěm pro archivaci dat jsou páskové knihovny.

3.3.5.3 Požadavky na zálohovací zařízení typu Disk-to-Disk

Zálohovací zařízení typu disk-to-disk bude sloužit pro zálohy celých virtuálních serverů, aplikací, databází i jednotlivých souborů, a to s důrazem na vysoký výkon zálohovacího řešení. Zařízení musí byt zcela kompatibilní se řídícím software potřebným pro realizaci záloh.

Číslo	Vlastnost/komponenta	Požadované minimální parametry
1.	Hrubá kapacita zálohovacího zařízení disk-to-disk	min. 480 TB
2.	Pordpora svazků RAID	RAID 0 RAID 1 RAID 10 RAID 5

Číslo	Vlastnost/komponenta	Požadované minimální parametry
		RAID 6
3.	Typ disku	7200 rpm, SAS nebo SATA rozhraní
4.	Velikost disku	4TB
5.	Počet řadičů úložných zařízení (SAN HBA)	min. 2 (redundantní provoz)
6.	SAN HBA - specifikace	min. 4x FC ports / 16Gb min. 2x 10 Gbit ethernet
7.	Velikost	max. 24U
8.	Počet napájecích zdrojů	min. 2 (redundantní provoz)
9.	Počet připojitelných hostů	min. 32

Tabulka č. 12 – požadavky na zálohovací zařízení D2D

Zařízení musí umožnovat vyčlenění části své kapacity i pro zálohování systémů Zadavatele prováděných na aplikační úrovni.

Zadavatel požaduje dodání 1 kusu zálohacího zařízení typu Disk-to-Disk (tabulka č. 12)

3.3.5.4 Požadavky na páskové jednotky

Páskové jednotky budou sloužit jako primární úložiště pro archivaci dat. Datové centrum musí být vybaveno min. 2 páskovými knihovnami se souhrnou kapacitou min. 240 slotů pro pásky typu LTO6. Každá pásková knihovna bude mít minimálně 2 zapisovací jednotky LTO6.

Na vzorovém schéma Datového centra (obrázek č. 2a,b) jsou zobrazeny 3 páskové knihovny, každá s kapacitou 80 slotů pro pásky LTO6, která je také přípustná.

Tabulka č. 13 udává minimální parametry jedné páskové knihovny.

Číslo	Vlastnost/komponenta	Požadované minimální parametry
1.	Počet slotů na pásky	80
2.	Typ pásky	LTO6 (2.5TB bez komprese)
3.	Počet páskových mechanik	2
4.	Nativní přenosová kapacita	100 MB/s
5.	Rozhraní	FC ports 8 Gb/s
6.	Velikost	max. 6U pro 80 slotů

Číslo	Vlastnost/komponenta	Požadované minimální parametry
7.	Počet napájecích zdrojů	min. 2 (redundantní provoz)
8.	Vzdálená správa	ano, vč. centrálního jednotného managementu pro všechny páskové knihovny
9.	Náhradní pásky	ke každé páskové knihovně musí být dodán dvojnásobný počet nových LTO6 pásek. Příklad: pásková knihovna s 80 slotů = dodat 160 pásek pásková knihovna s 120 sloty = dodat 240 pásek

Tabulka č. 13 – požadavky na jednu páskovou jednotku

3.3.6 Požadavky na datové rozvaděče a podružný materiál

Datové rozvadeče musí být minimální výšky 42U a šíře 600mm (případně maximálně 2 datové rozvaděče mohou být i šíře až 800mm).

Hloubka datových rozvaděčů musí umožnovat bezproblémovou instalaci veškerého hardware a přehlednou instalaci veškeré kabeláže.

Součástí datových rozvaděčů musí být veškeré potřebné příslušenství (kabeláž, PDU), a to v potřebném množství. Datové rozvadeče musí být uzamykatelné.

V každém datovém rozvaděči musí být k dispozici zařízení ATS (Automatic transfer switch) umožnující spolehlivé redundantní napájení pro zařízení s jedním napájecím zdrojem.

Zadavatel v rámci součinnosti poskytne Uchazeči ke každému datovému rozvaděči max. 4 zásuvky na elektrickou energii. Veškerá ostatní příslušenství (potřebná kabeláž, aktivni í pasivní prvky) musí být součástí dodávky Datových center.

3.4 Monitorovací systém DDC

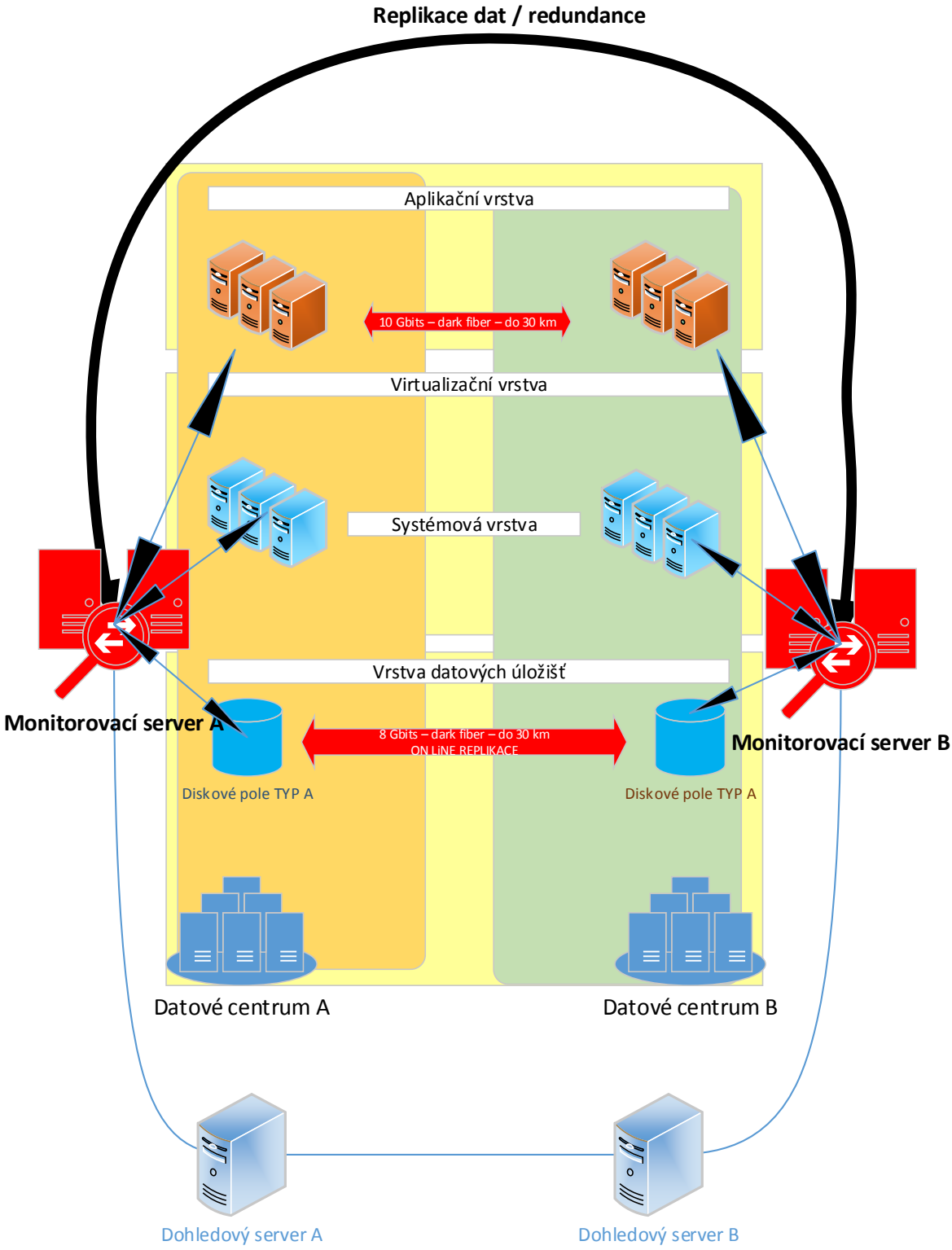
Zadavatel požaduje dodání monitorovacího systému DDC. Monitorovací systém zajistí monitorování všech jednotlivých prvků obou Datových center vč. provozovaných virtuálních serverů a jednotlivých technologických služeb. Monitorovací systém bude sloužit jako primární nástroj pro sledovaní provozních stavů jednotlivých prvků DDC.

Monitorovací systém se skládá z:

- specializovaný SW pro monitoring,
- HW Infrastuktura.

SW použitý pro monitoring nesmí být typu open-source bez podpory výrobce.

Monitorovací systém bude tvořen dvěmi monitorovacími servery, které budou vzájemně zastupitelné (redundance). Taktéž bude možno redundantně monitorovat technologické služby DDC ze dvou různých lokací (umístění monitorovacích serverů). Správa monitorovacího systému bude možná prostřednictvím webového prohlížeče.



Obrázek č. 9 – schéma monitorovacího systému

Monitorovací systém musí umožnovat monitorování minimálně 200 typů technologických služeb, bezvýhradně však musí spolupracovat s dodaným HW DDC. Dále musí být schopen monitorovat zejména tyto technologické služby:

- http sensor,
- Ping sensor,
- Port sensor,

- Port range sensor,
- SNMP traffic sensor,
- SSL security check sensor,
- Windows Network Card sensor,
- SNMP RMON sensor,
- SNMP traffic sensor,
- NetFlow V5,
- NetFlow V9,
- WMI Microsoft SQL Server 2005 Sensor,
- WMI Microsoft SQL Server 2008 Sensor,
- WMI Microsoft SQL Server 2012 Sensor,
- WMI Microsoft SQL Server 2014 Sensor,
- WMI Share Sensor,
- WMI SharePoint Process Sensor,
- WMI Terminal Services (Windows 2008) Sensor,
- SNMP Linux Disk Free Sensor,
- SNMP Linux Load Average Sensor,
- SNMP Linux Meminfo Sensor,
- SNMP Linux Physical Disk Sensor,
- SSH Disk Free Sensor,
- SSH INodes Free Sensor,
- SSH Load Average Sensor,
- SSH Meminfo Sensor,
- SSH Remote Ping Sensor,
- SSH Script Sensor,
- SSH Script Advanced Sensor,
- SSH SAN Enclosure Sensor,
- SSH SAN Logical Disk Sensor,
- SNMP Linux Disk Free Sensor,
- SNMP Linux Load Average Sensor,
- SNMP Linux Meminfo Sensor,
- SNMP Linux Physical Disk Sensor,
- SSH Disk Free Sensor,
- SSH INodes Free Sensor,
- SSH Load Average Sensor,
- SSH Meminfo Sensor,
- SSH Remote Ping Sensor,
- SSH Script Sensor,
- SSH Script Advanced Sensor,
- SSH SAN Enclosure Sensor,
- SSH SAN Logical Disk Sensor,
- DHCP Sensor,
- DNS Sensor,
- LDAP Sensor,
- Ping Jitter Sensor,
- Pingdom Sensor,
- Port Range Sensor,
- RADIUS Sensor,
- RADIUS v2 Sensor,
- RDP (Remote Desktop) Sensor,
- SNMP Trap Receiver Sensor,
- SNTP Sensor,
- SSL Security Check Sensor.

Monitorovací systém nesmí být omezen počtem monitorovaných technologických služeb z hlediska licence. Systém musí být schopen monitorovat více než 6000 hodnot.

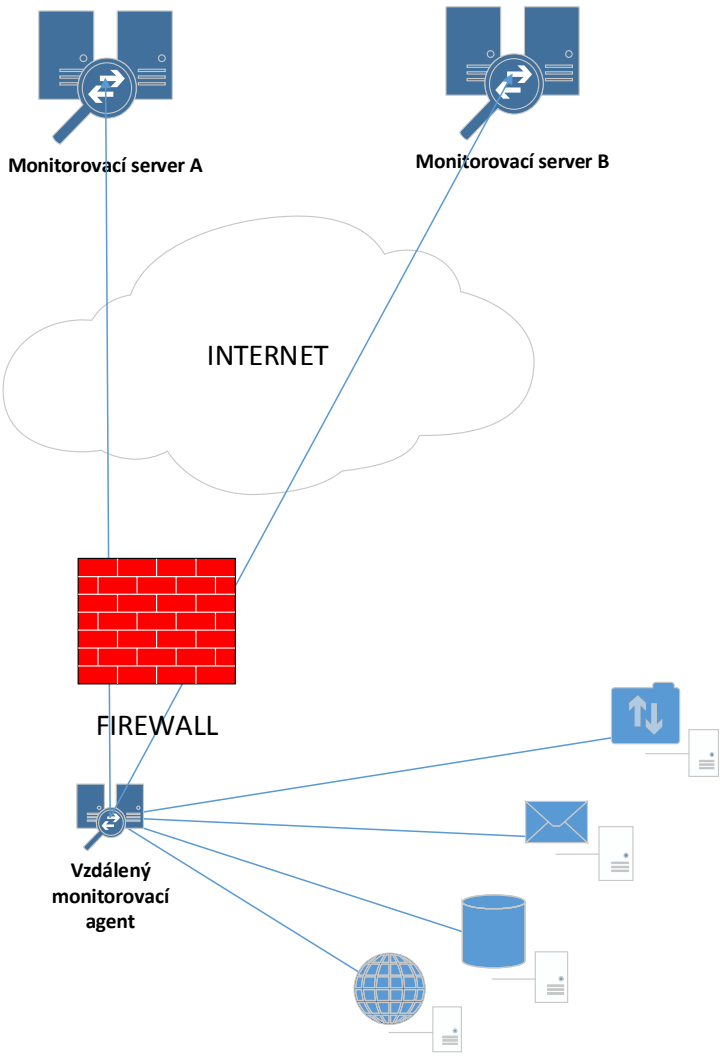
Monitorovací systém poskytuje následující funkcionality:

- sběr a uchování naměřených údajů (provozních stavů),
- posílání chybových zpráv formou SMS, emailu a záznamů do Service Desku zadavatele,
- poskytování uceleného přehledu o funkčnosti DDC (manažerský přehled),
- přistup přes webové rozhraní,
- vytváření ucelných reportů za předem definované časové období.

Monitorovací systém musí být implementován takovým způsobem, aby byl rozšířitelný i na servery a jiné aktivní prvky mimo datové centrum.

Monitorovací systém musí být řešen redundantně, neboť bude sloužit jako primární nástroj pro odhalení nefunkčnosti systémů (proaktivní monitoring).

Monitorovací systém musí umožnovat instalaci vzdálených uzlů (agentů), umožnující monitorování vzdálené části sítě, která není dosažitelná pro monitorovací servery A a B.



Obrázek č. 10 – schéma monitorovacího systému s 1 vzdáleným agentem (remote probe)

3.4.1 Požadavky na hardware

Zadavatel vyčlenil pro monitorovací systém v každém Datovém centru 1ks server – TYP C (tabulka č. 7) .

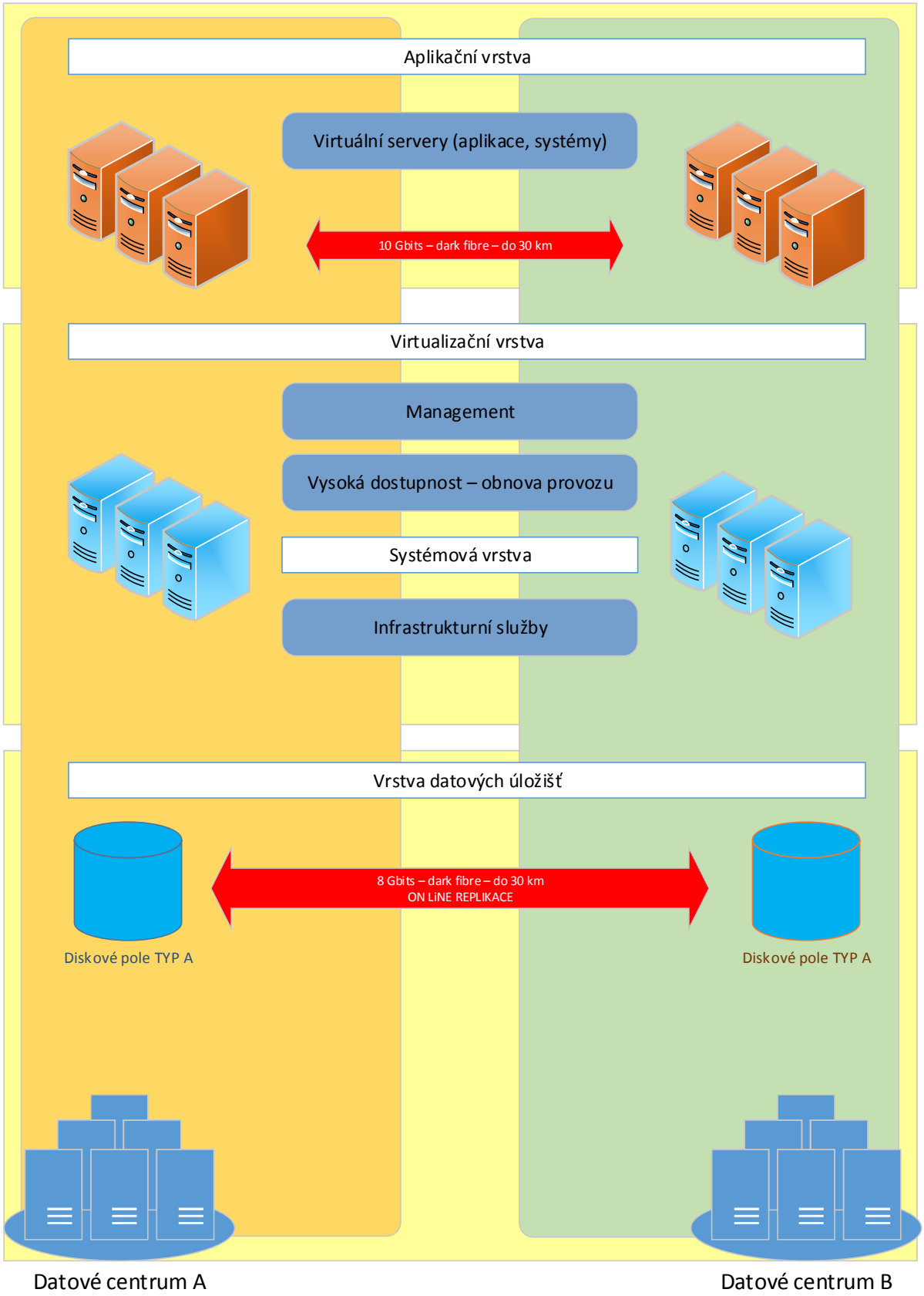
3.5 Požadavky na funkcionalitu Datových center

V rámci datového centra bude provozována jednotná virtualizační platforma Microsoft Hyper-V. Virtualizační platforma bude rozdělena do několika na sobě nezávislých virtualizačních clusterů. Maximální počet clusterů bude 10 v rámci jednoho Datového centra.

Zadavatel požaduje rozčlenění DDC na jednotlivé clustery:

- provozované aplikace vyžadují zalicencovat veškerý hardware dostupný v rámci clusteru,
- fyzické oddělení provozu aplikací.

Pro vysokou dostupnost všech aplikací budou obě Datová centra přístupná z komunikační infrastruktury a budou transparentní, tj. pro uživatele aplikací/služeb bude neviditelné, z kterého datového centra je aplikace repektivě služba poskytována.



Obrázek č. 11 – schéma Datových center

3.5.1 Požadavky na virtualizační clustery

Virtualizační clustery budou tvořeny několika fyzickými servery. Cluster musí umožnovat provoz virtuálních serverů v režimu vysoké dostupnosti a dále musí umožnovat tyto funkce:

Číslo	Název	Popis
1.	Sdílený virtuální disk	Tato funkce slouží k vytvoření infrastruktury s vysokou dostupností a zvlášť důležitá je pro nasazení privátních cloudů a prostředí hostovaných v cloudu, která spravují rozsáhlejší úlohy. Sdílené virtuální pevné disky umožňují několika virtuálním počítačům přistupovat ke stejnému souboru virtuálního pevného disku (VHDX), který poskytuje sdílené úložiště používané Clusteringem Windows s podporou převzetí služeb při selhání. Soubory sdílených virtuálních pevných disků se dají hostovat na sdílených svazcích clusteru (CSV) nebo ve sdílených složkách souborového serveru se škálováním na víc systémů založeného na protokolu SMB (Server Message Block).
2.	Změna velikosti virtuálního pevného disku	Změna velikosti virtuálních pevných disků při spuštěném virtuálním počítači umožňuje správci provádět operace konfigurace a údržby na virtuálních pevných discích, zatímco přidružený virtuální počítač je online nebo se data virtuálního pevného disku zrovna používají.
3.	QoS pro úložiště	Technologie QoS úložiště umožňuje určit maximální a minimální zatížení vstupu a výstupu jako počet vstupních a výstupních operací za sekundu (IOPS) pro každý virtuální disk na vašich virtuálních počítačích. Technologie QoS úložiště zajišťuje, aby propustnost úložiště jednoho virtuálního pevného disku neměla vliv na výkon jiného virtuálního pevného disku na stejném hostiteli.
4.	Migrace za provozu	U nasazení větších měřítek, třeba u nasazení privátních cloudů nebo poskytovatelů cloudových hostitelských služeb, může tato aktualizace snížit režijní náklady na síť a využití procesoru. Navíc snižuje množství času potřebného k migraci za provozu. Správci Hyper-V můžou nakonfigurovat příslušné možnosti výkonu migrace za provozu na základě jejich prostředí a požadavků (TCP/IP, SMB 3.0, komprese)
5.	Migrace za provozu napříč verzemi	Administrátor Hyper-V můžou přesunout virtuální počítače s Hyper-V v systému Windows Server 2012 na technologii Hyper-V v systému Windows Server 2012 R2 nebo novějším. Přesunutí virtuálního počítače na server nižší úrovně s Hyper-V se nepodporuje.
6.	Volba generace virtuálního serveru	**Generace 1:** Poskytuje virtuálnímu počítači stejný virtuální hardware jako předchozí verze technologie Hyper-V. **Generace 2:** Poskytuje virtuálnímu počítači následující nové funkce: • zabezpečené spouštění (povolené ve výchozím

Číslo	Název	Popis
		nastavení), • spouštění z virtuálního pevného disku SCSI, • spouštění z virtuálního disku DVD SCSI, • spouštění pomocí technologie PXE s použitím standardního síťového adaptéru, • podpora firmwaru UEFI.
7.	Export virtuálního serveru	• Administrátor může exportovat virtuální počítač, který je spuštěný, aniž by docházelo k výpadkům. o Duplikování existujícího provozního prostředí nebo části prostředí do testovací laboratoře. o Testování plánovaného přesunu do privátního cloudu nebo poskytovatele cloudových hostitelských služeb. o Odstraňování potíží s aplikacemi.
8.	Clustering s podporou převzetí služeb při selhání	Cluster umožnuje rozpoznání chyby fyzické paměti u paměťových zařízení (fyzický disk apod.). Pokud k takové události dojde, Clustering s podporu převzetí převzetí služeb při selhání zajistí přemístění a restartování virtuálního počítače v jiném uzlu clusteru. Omezí se tak případy, ve kterých by se chyby nespravovaného úložiště nerozpoznaly a prostředky virtuálního počítače se mohly stát nedostupnými
9.	Replikace virtuálních serverů	Lze nastavit frekvenci replikací viruálních serverů. Replikace probíhá mezi Hyper-V servery
10.	Automatická aktivace virtuálních serverů	Automatická aktivace virtuálního počítače (AVMA) umožňuje nainstalovat virtuální počítače na počítači se správně aktivovaným systémem Windows Server 2012 R2. Nemusíte spravovat kódy Product Key pro každý virtuální počítač zvlášť (ani v odpojených prostředích). Automatická aktivace virtuálního počítače váže aktivaci virtuálního počítače na licencovaný server virtualizace a aktivuje virtuální počítač po jeho spuštění. Automatická aktivace virtuálního počítače poskytuje taky sestavy o využití v reálném čase a historická data týkající se stavu licence virtuálního počítače. Generování sestav a sledování dat je k dispozici na serveru virtualizace.
11.	Virtuální komunikační infrastruktura	Možnost zřízení virtuální VLAN, FC SAN. Oddělení provozovaných virtuálních serverů z hlediska bezpečnosti na úrovni komunikační infrastruktury.

Číslo	Název	Popis
12.	Energetická úspornost	Virtualizační servery budou provozovány v takovém počtu, aby byl zajištěn požadovaný výkon. Virtualizační servery poskytující nadbytečný výkon budou vypnuty nebo převedeny do režimu spánku. Aktivace serverů bude provedena automaticky, jakmile bude překročena stanovená mez využití clusteru.

Tabulka č. 14 – požadavky na virtualizační cluster

Zadavatel dále přepokládá využití všech funkcí, které platforma Microsoft Hyper-V poskytuje a bude v budoucnu poskytovat.

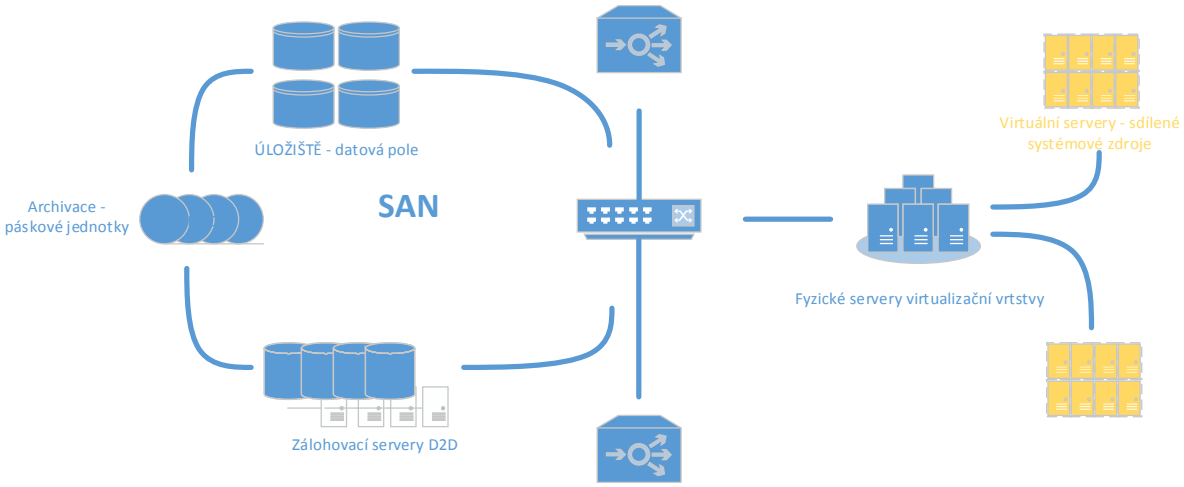
Virtualizační cluster musí umožňovat jak rezervaci, tak sdílení systémových zdrojů (výkon CPU, RAM, výkon diskového subsystému) pro provozované virtuální servery, takovým způsobem, aby byl provozovaný hardware optimálně využit.

Prostředí musí umožnovat kategorizaci virtuálních serverů z hlediska využití systémových zdrojů do min. 3 skupin:
CAT. 1 – vyhrazený procesorový výkon, operační paměť, diskový subsystém (QoS),
CAT. 2 – sdílený procesorový výkon a operační paměť s vysokou prioritou,
CAT. 3 – sdílený procesorový výkon a operační paměť s nízkou prioritou nebo dynamicky přidělovanou.

Virtuální servery mohou být migrovány napříč jednotlivými clustery nebo jednotlivými Datovými centry, a to v závislosti na provozních a technických požadavcích Zadavatele.

3.5.2 Požadavky na virtuální servery

Virtuální server musí být provozován v rámci virtualizačního clusteru. Data jsou uložena na sdíleném diskovém poli a diskových svazcích zajišťujících odolnost proti selhání fyzického disku.



Obrázek č. 12 – virtuální servery

Virtuální server bude provozován s operačními systémy podporovanými virtualizační platformou Microsoft Hyper-V. Virtuální server musí splňovat tyto výkononstní parametry:

- konektivita do komunikační infrastruktury 100 – 10 000 mbps,
- možnost alokace 1 – 42 procesorových jader,
- možnost alokace až 640 GB operační paměti,
- možnost alokace diskového úložiště na bázi SSD, SAS, SATA vč. jejich kombinace,
- provoz v režimu vysoké dostupnosti (online migrace mezi fyzickými servery, datovými poli),
- možnost provozu v režimu vyhrazených nebo sdílených systémových prostředku clusteru,
- možnost přímého přístupu diskovým polím pomocí iSCSI, FCoE nebo obdobné technologie.

3.6 Dohledové centrum

Zadavatel požaduje vybudování jednotného administračního rozhraní pro správu a monitoring Infrastruktury - konfigurací, správu úloh (jobů) a jejich plánování (generování výstupných sestav, správu oprávnění - které bude umístěno v lokalitě Datového centra B (dále také jen jako „Dohledové centrum“). Dohledové centrum bude sloužit jako jediné místo pro tuto správu a monitoring Infrastruktury. Schéma Dohledového centra je uvedeno na obrázku č. 13. Dohledové centrum bude nezávislé na virtuzalizační platformě DDC.

Dohledové centrum bude tvořeno:

- servery dohledového centra (dohledový server A, dohledový server B),
- koncové počítače dohledového centra,
- technologií pro zajištění vzdáleného přístupu,
- integrace monitorovacího systému.

Z hlediska komunikační infrastruktury bude umožněn přístup z Dohledového centra do všech částí komunikační infrastruktury a v takovém rozsahu, aby mohla být prováděna správa všech aktivních prvků (servery, switche, FC technologie, disková pole) datových center.

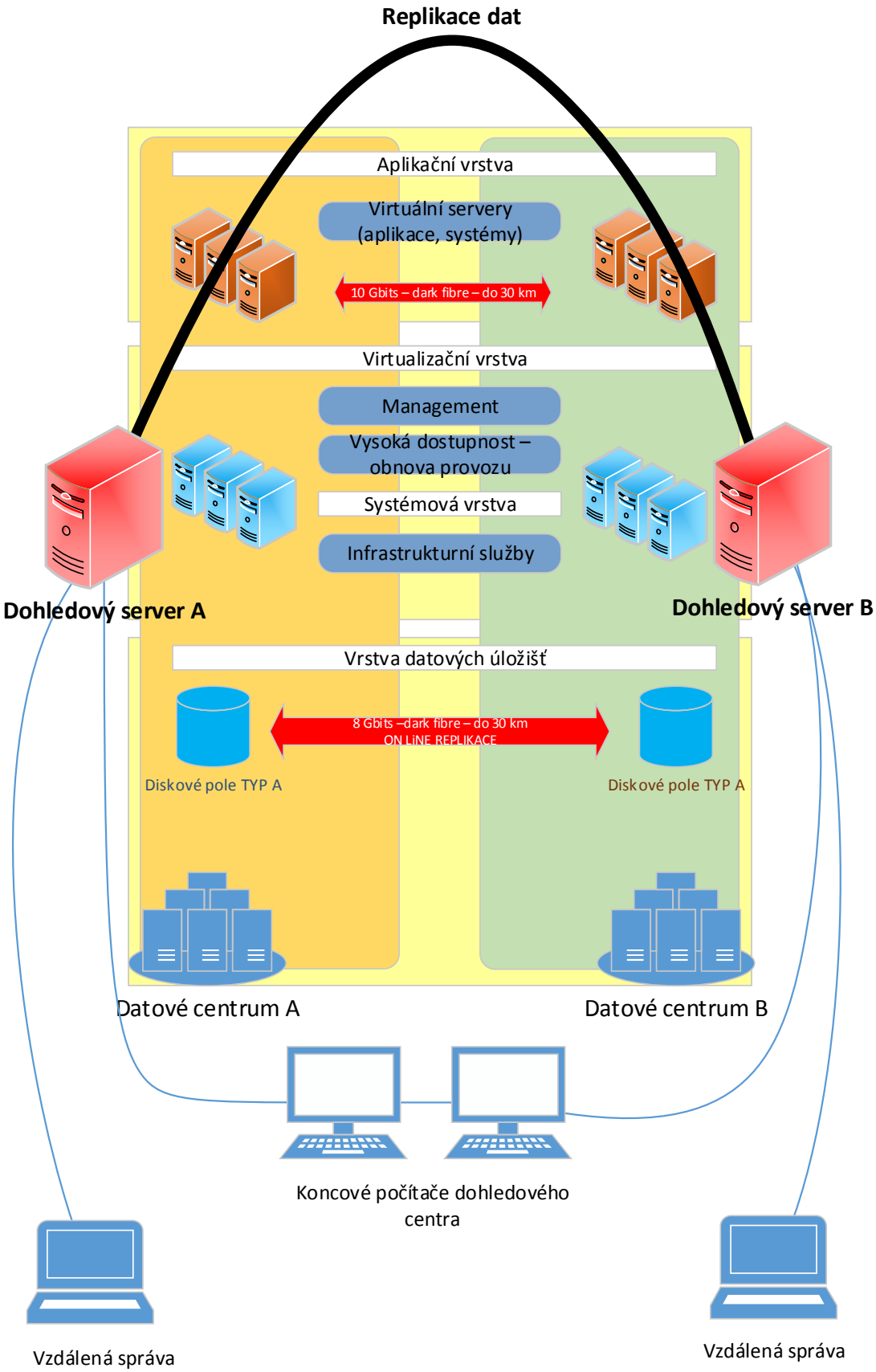
Veškerá správa prvků DDC bude prováděna prostřednictvím dohledových serverů A a B, na kterých musí být k dispozici veškerý potřebný SW pro tuto činnost.
Dohledové servery A a B budou zároveň sloužit i jako centrální úložitě veškeré dokumentace (provozní, technická, servisní) včetně dokumentace pro řádné obnovení provozu. Požadavky na dokumentaci jsou uvedeny v kapitole 3.10.
V rámci dohledového serveru může být aktivována virtualizační technologie Hyper-V a server může sloužit jako virtualizační, avšak pouze pro SW a technologické služby související s chodem Dohledového centra (např. dedikovaný VPN server apod.).

Přístup na dohledové servery A a B server bude umožněn:

- lokálně přes LCD s integrovanou klávesnicí a myší v rámci datového centra,
- z koncových počítačů dohledového centra umístěne ve vyhrazené místnosti DC SOK za pomocí služby RDP,
- z mobilních počítačů vzdálenou formou za pomocí virtuálního privátního spojení a služby RDP a to prostřednictvím VPN.

Všechny prvky Dohledového centra musí být v rámci jedné dedikované VLAN, ze které bude umožněn plný přístup do ostatních částí komunikační infrastruktury DDC.

Součástí vyhrazené sítě Dohledového centra budou dedikované servery pro monitoring (viz. kapitola 3.4).



Obrázek č. 13 – schéma Dohledového centra

3.6.1 Požadavky na dohledové servery

Zadavatel požaduje minimální závislost dohledového serveru na vlastních Datových centrech. Z tohoto důvodu má dohledový server vlastní storage. K dohledovému serveru bude připojen externí LCD s integrovanou klávesnicí a myší. Požadavky na dohledový server jsou uvedeny v tabulce č.15. Každé Datové centrum bude vybaveno 1 dohledovým serverem.

Číslo	Vlastnost/komponenta	Požadované minimální parametry
1.	Počet CPU	1
2.	Výkon jednoho procesoru (body dle výkonnostního indexu www.passmark.com)	15 000
3.	Provedení	RACK - velikost do 3U a to vč. externího LCD s integrovanou klávesnicí a myší
4.	Napájení	redundantní napájecí zdroje (min. 2)
5.	Rodina procesoru	x-86 (podpora 64bit)
6.	Počet pevných disků	8
7.	Kapacita a typ pevného disku	600 GB SAS 10K
8.	RAM	48 GB
9.	SAN HBA	2x16Gb (2x single-port HBA)
10.	LAN	4x 10Gb
11.	Plně 64bit HW a SW architektura	požadováno
12.	Hardwarová akcelerace šifrování AES	požadováno
13.	Vzdálený management	KVM, console, virtual media
14.	Zobrazovací jednotka	LCD display umístitelný do RACK rozvadeče vč. integoravné klávesnice a myši nebo touchpadu. Rozlišení LCD 1366x768 a více

Tabulka č. 15 – požadavky na dohledový server

3.6.2 Požadavky na koncové počítače dohledového centra

Počítače budou umístěny ve vyhrazené místnosti DC SOK (dohledové centrum). Počítače budou sloužit ke správě a údržbě datových center. Počítače musí být vybaveny potřebnými porty pro správu jednotlivých prvků. Jedná se zejména o COM porty, potřebné pro nastavování aktivních prvků datových center na nejnižší úrovni.

V rámci dohledového centra budou k dispozici 2 ks totožných počítačů splňující požadavky na minimální konfiguraci uvedené v tabulce č. 16.

Číslo	Vlastnost/komponenta	Požadované minimální parametry
1.	Počet CPU	1
2.	Výkon jednoho procesoru (body dle výkonnostního indexu www.passmark.com)	6 000
3.	Provedení	bez omezení

Číslo	Vlastnost/komponenta	Požadované minimální parametry
4.	Porty	min. 4x USB 2.0, 2x USB3.0, 1x COM port
5.	Rodina procesoru	x-86 (podpora 64bit)
6.	Počet pevných disků	1
7.	Kapacita a typ pevného disku	1x 120GB SSD 1x 4TB HDD
8.	RAM	16 GB
9.	LAN	1x 1Gb
10.	Zobrazovací jednotka	LCD 24“, rozlišení min. FULL HD, výškově stavitelný
11.	Plně 64bit HW a SW architektura	požadováno

Tabulka č. 16 – požadavky na koncové počítače dohledového centra

3.6.3 Požadavky na zajištění vzdáleného přístupu

Vzdálený přístup k dohledovému centru bude zřízen formou VPN spojení. V případě potřeby bude realizován VPN tunel mezi dohledovým centrem a síti dodavatele.

U vybraných mobilních uživatelů bude přístup umožněn formou VPN spojení klient-server ze sítě Internet. Pro realizaci VPN spojení lze využít buď centrálních hraničních prvků v rámci D
Datových center, nebo bude Uchazečem implementováno proprietální softwarové řešení, závislé pouze na hardware náležící do dohledového centra.

3.7 Dodávka hardware a software

Dodávkou HW a SW se rozumí dodání veškerého zařízení a software, jehož minimální požadavky (parametry) určuje tato Zadávací dokumentace. Zadavatel zejména požaduje:

- dodržení požadavků na kompatibilitu uvedených v jednotlivých částech této Zadávací dokumentace,
- dodání HW a SW v požadovaném množství a konfiguraci,
- doručení HW a SW do prostor určených zadavatelem,
- příslušenství, které tato Zadávací dokumentace nemusí výslovně specifikovat, ale jsou nezbytné k řádnému zprovoznění dodávaného HW a SW a jeho optimálnímu provozu (mj. napájecí kabely, adaptéry, propojovací kabely mezi servery a LAN a SAN switchi, případně další nezbytné síťové i jiné komponenty). Za kompletnost Dodávky včetně veškerého potřebného příslušenství je plně odpovědný výhradně Uchazeč,
- dodržení milníků plnění uvedených v této Zadávací dokumentaci a podrobného časového harmonogramu, který bude schválen v rámci Technického projektu.

3.8 Implementace

3.8.1 Instalace a zprovoznění

Implementací se rozumí komplexní poskytnutí služeb v potřebném rozsahu související s instalací a konfigurací DDC.

V rámci Implementace bude Uchazečem zejména provedeno:

- fyzická instalace, zapojení dle schémat uvedených v této dokumentaci, (uvedení do řádného provozu) požadovaného hardware vč. řídícího software, dalšího potřebného příslušenství,
- zprovoznění jednotlivých prvků (ověření funkčnosti, aktuálnosti firmware, nastavení práv na úrovni hardware),
- instalace a následná konfigurace všech softwarových komponent,
- instalace virtualizační platformy vč. všech souvisejících služeb (centralizovaný management, podpůrné a servisní moduly),
- konfigurace virtualizační platformy (služby vysoké dostupnosti, úspory elektrické energie, nastavení práv),
- zřízení požadovaných rolí pro potřeby kontrolní nebo správní činnosti MPSV:
    - Administrátor - přístup do všech systémů vč. aktivních prvků s právy bez omezení.
    - Operátor virtuálních strojů - možnost vytvářet virtuální servery v rámci datového centra, měnit jejich parametry. Vše do té míry, aby nebyl ohrožen provoz služeb.
    - Dohledový manažer – přístup k veškeré dokumentaci, přístup do všech systémů avšak s právy pouze pro čtení.

- Nastavení optimální výkonosti virtualizační platformy - disková pole, switche, servery,
- nastavení energetické efektivity – servery poskytující nadbytečný výkon budou automaticky zapnuty/vypnuty v souladu s požadavky na aktuální potřebu výkonu,
- dílčí ověření funkčnosti virtualizační platformy,
- provedení dokumentace platformy - zejména nastavení, komunikační schéma servery vs. datové pole,
- implementace monitoringu – dohledový systém,
- zřízení, instalace a konfigurace dohledového centra,
- registrace SW, zejména licencí na Zadavatele,
- instalace a konfigurace datových úložišť,
- konfigurace SAN,
- konfigurace diskových polí dle Best Practices a Technického plánu,

- konfigurace diskových prostor na datových úložištích,
- konfigurace napojení datových úložišť na virtualizační servery,
- implementace monitoringu,
- nastavení replikace mezi diskovými poli umístěnými ve vzdálených lokalitách,
- nastavení a ověření funkčnosti replikace 1:1 mezi poli,
- implementace zálohování,
- dokumentace instalovaného prostředí datových úložišť,
- zpracování detailní dokumentace technického řešení DDC vč. podrobných schémat zapojení (popis adresních prostorů, popis kabeláže, modulů, aktivních prvků na úrovni portů ……). Výstupem bude tištěná i elektronická dokumentace. Tištěná dokumentace bude umístěna v prostorách každého Datového centra,
- provedení funkčních, bezpečnostních, penetračních a zátěžových testů každého Datového centra samostatně,
- optimalizace implementované instalace a konfigurace každého Datového centra samostatně,
- předání do ověřovacího provozu každého Datového centra samostatně.

3.8.2 Ověřovací provoz Datového centra A

Zadavatel požaduje zajištění ověřovacího provozu Datového centra A v následujícím rozsahu:

- poskytování Služeb podpory provozu v rozsahu KS1.1 Podpora provozu komponenta „Řešení incidentů“ bez požadovaných lhůt pro poskytování Služby (SLA),
- poskytování Služeb podpory provozu v rozsahu KS1.4 Podpora provozu komponenta „Bezpečnostní dohled“ bez požadovaných lhůt pro poskytování Služby (SLA),
- realizace Technických činností v rozsahu požadovaném Zadavatelem,
- délka ověřovací provozu Datového centra A bude dle Harmonogramu.

3.8.3 Ověřovací provoz Datového centra B

Zadavatel požaduje zajištění ověřovacího provozu Datového centra B v následujícím rozsahu:

- poskytování Služeb podpory provozu v rozsahu KS1.1 Podpora provozu komponenta „Řešení incidentů“ bez požadovaných lhůt pro poskytování Služby (SLA),

- poskytování Služeb podpory provozu v rozsahu KS1.4 Podpora provozu komponenta „Bezpečnostní dohled“ bez požadovaných lhůt pro poskytování Služby (SLA),
- realizace Technických činností v rozsahu požadovaném Zadavatelem,
- délka ověřovací provozu Datového centra B bude dle Harmonogramu,
- příprava integračních a akceptačních testů DDC,
- předání DDC k akceptaci.

3.8.4 Akceptace DDC

Závěr Implementace bude ukončen akceptačními testy DDC, při kterých bude ověřena celková funkčnost DDC a odolnost proti nahodilým výpadkům.

3.9 Ostatní činnosti

3.9.1 Konzultační činnosti

Zadavatel požaduje poskytnutí konzultačních činností IT specialistů dle požadavků Zadavatele po celou dobu účinnosti Smlouvy a v rozsahu 800 MD, a to na základě požadavků Zadavatele učiněných postupem uvedeným ve Smlouvě.

Konzultační činnosti je Zadavatel oprávněn využít i pro migraci systémů a dat Datových center do jiných lokalit, lze je využít i pro optimalizaci migrovaných systémů a dat, přípravu a konfiguraci prostředí pro dodavatele aplikací/systémů a další součinnosti.

3.9.2 Technologické činnosti

Zadavatel požaduje poskytnutí technologických činností uvedených v následující tabulce, které bude Uchazeč poskytovat na základě požadavku Zadavatele po celou dobu účinnosti Smlouvy, a to na základě požadavků Zadavatele učiněných postupem uvedeným ve Smlouvě.

Technoligické činnosti spočívají v provádění níže definovaných úkonů:

ID	Název a popis úkonu	Maximální počet úkonů
ÚKON 1	**Zřízení virtuálního serveru** Popis: - vytvoření virtuálního serveru (VS) na základě požadavků zadavatele na virtualizační platformě zadavatele, - instalace operačního systému v rámci zřízení VS (Linux	400

	nebo Windows), vč. přiřazení IP adresy, aplikace všech dostupných bezpečnostních záplat a vytvoření uživatelských účtů (max. 10 účtů), - přiřazení VS do patřičné VLAN vč. nastavení firewallu dle požadavku, - aktivace dohledového systému (max. 15 technologických služeb).	
ÚKON 2	**Zálohování virtuálního serveru** Popis: - nastavení obsahu a typu zálohování pro virtualizační servery, na kterých jsou provozované aplikace třetích stran, (jednorázové, přírůstkové,…) na základě požadavků zadavatele.	400
ÚKON 3	**Změna parametrů virtuálního serveru** Popis: - změna parametrů, tj. nastavení RAM, HDD, vCPU a priority systémových zdrojů na základě požadavku zadavatele, - změna VLAN, - změna clusteru nebo diskového úložiště, - konfigurace firewallu, - pořízení/smazání snapshotu, - změna monitorovacího systému (doplnění/smazání), senzoru (max. 15 technologický služeb). Všechny výše uvedené činnosti budou vykonávány na virtuálních serverech, na kterých jsou provozované aplikace třetích stran.	600
ÚKON 4	**Zrušení virtuálního serveru** Popis: - archivace celého virtuálního serveru před jeho zrušením, - zrušení VS**,** odstavení VLAN a všech nastavení, uvolnění IP, nastavení firewalu pro virtuální servery, na kterých jsou provozované aplikace třetích stran.	40
ÚKON 5	**Import VS – typ P2V (physical to virtual)** Popis: - migrace fyzického serveru do virtualizační platformy, - přiřazení VS do patřičné VLAN vč. nastavení firewallu dle požadavku zadavatele, přiřazení IP adres, - aktivace monitorovacího systému (max. 15 technologických služeb). Všechny výše uvedené činnosti budou vykonávány	150

	na virtuálních serverech, na kterých jsou provozované aplikace třetích stran.	
ÚKON 6	**Import VS – typ V2V (virtual to virtual)** - migrace virtuálního serveru do virtualizační platformy, - přiřazení VS do patřičné VLAN vč. nastavení firewallu dle požadavku, přiřazení IP, - aktivace dohledového systému (max. 15 technologických služeb), - virtuální server bude pro uložení připraven v běžně užívaném formátu pro export/import virtuálních serverů. Všechny výše uvedené činnosti budou vykonávány na virtuálních serverech, na kterých jsou provozované aplikace třetích stran.	350

3.10 Technická a systémová dokumentace

3.10.1 Technický projekt

Technickým projektem se rozumí vytvoření konceptu DDC na základě požadavků uvedených v této Zadávací dokumentaci. Uchazeč v rámci plnění zpracuje podrobný technický popis řešení dodané Infrastruktury, kterou bude Implementovat.

Součástí bude i projektový plán, dokumentace a detailní harmonogram.

Uchazeč současně předloží návrhy testovacích scénářů pro akceptaci řešení Zadavatelem.

Technický projekt musí obsahovat:

- navržené schéma Infrastruktury,
- deklarovaná energetická úspornost a efektivita,
- odolnost proti výpadku – redundance (vysoká dostupnost),
- detailní popis HW a SW (vč. kapacitních a výpočetních hodnot),
- podrobný harmonogram dodávek HW a SW na jednotlivá Datová centra v souladu se závaznými milníky uvedenými v Zadávací dokumentace,
- časový harmonogram Implementace jednotlivých Datový center včetně souvisejících činností realizace DDC,
- definice komunikačních kanálů ServiceDesk,
- jmenný seznam osob Uchazeče podílejících se na plnění předmětu Smlouvy, včetně odpovědností - komunikační matice,

- definici případných standardních softwarových produktů Uchazeče nebo třetích osob, které budou tvořit součást Dodávky, včetně licenčních podmínek, za kterých budou příslušné softwarové produkty Zadavateli poskytnuty,
- specifikace SW a licenčních požadavků MS na Zadavatele při implementaci virtualizační platformy Microsoft Hyper-V,
- vymezení požadavků na součinnost Zadavatele a případných třetích stran při realizaci Dodávky,
- případné další otázky a skutečnosti, jejichž specifikace je pro realizaci Dodávek nezbytná,
- návrh testovacích scénářů.

3.10.2 Bezpečnostní projekt

V rámci této etapy bude vytvořen dokument Bezpečnostní projekt, který bude obsahovat zejména:

- návrh pravidel pro bezpečnostní audit Infrastruktury v souladu s příslušnými předpisy,
- návrh procesů a pravidel v rozsahu pro poskytování Služby KS1.4 Bezpečnostní dohled.

3.10.3 Ostatní dokumentace

Zadavatel požaduje zpracování **Zálohovacího plánu**. Zálohovací plán bude obsahovat zejména:

- identifikace datových aktiv (systémový SW),
- identifikace datových aktiv JISPSV (všechny agendové a podpůrné systémy),
- stanovení maximální doby ztráty dat,
- definice zálohovacích postupů pro poskytování Služby KS1.6 Záloha a obnova.

Speciální oblastí, která bude podléhat zvýšené pozornosti při přípravě zálohovacího plánu a následně kontrole záloh v rámci poskytování Služby KS1.6, je datová oblast pro logy. Zadavatel požaduje, aby zálohovací plán respektoval požadavek na dlouhodobou archivaci logů tak, aby bylo možné dohledat potřebné auditní údaje v dlouhodobém horizontu. Stanovení konkrétních lhůt pro archivaci a zálohu bude provedeno při přípravě Zálohovacího plánu a lze očekávat, že bude v řádu měsíců, popřípadě let.

Zadavatel dále požaduje zpracovat také následující technickou a systémovou dokumentaci:

- **Recovery plán** - včetně návrhu testu obnovy,
- **Dokument matice závislostí DDC** – obsahuje matici závislostí prvků obsažených v Datových centrech, jejich jejich vlivu na dostupnost Infrastruktury a vazby na monitoring,
- **Havarijní plán a plán kontinuity služeb** - dokument popisující předem ověřené postupy, při selhání určitě části datového centra,
- **Analýza rizik,**

- **Provozní příručka** - zapisují se zde všechny podstatné události (úprava, aktualizace, servisní úkon). Provozní dokumentace musí být vedena ke každému aktivnímu prvku (switch, router, server, firewall, diskové pole), a to v takovém rozsahu, aby bylo možno dohledat jaké úkony, kdy a kým byly prováděny,
- **Bezpečnostní deník** – zapisují se zde veškeré incidenty bezpečnostního charakteru,
- **Uživatelský manuál,**
- součinnost při zpracování **Plánu odstávek**,
- **Dokumentace pro administrátory.**

Technická a systémová dokumentace, která obsahuje veškeré technické informace o Datových centrech a jeho dílčích částech (komunikační infrastruktura, virtualizační platforma, disková pole, zálohování apod.), musí být v průběhu plnění Smlouvy udržována a aktualizována. Součástí musí být také schémata zapojení, popisy na úrovni aktivních prvků, související příručky a manuály. Součástí dokumentace musí být i veškeré relevantní podružné soubory, jako jsou např. konfigurační soubory k jednotlivým prvkům Datových center, firmware.

Primární úložiště dokumentace bude součástí dohledového centra. Zadavatel požaduje zřízení jednotného úložšitě na platformě Microsoft SharePoint (Foundation). Úložiště musí být replikováno mezi dohledovým server A a B pro zajištění vysoké dostupnosti a odolnosti proti výpadku. Metodika verzování dokumentů bude schválena v rámci Technického projektu. Úložiště musí umožnovat přístup administrátorů a oprávněných osob Zadavatele prostřednictvím internetového prohlížeče a zároveň umožnovat ukládání dat libovolného formátu (konfigurační soubory aktivních prvků, firmware a jiné).

3.10.4 Požadavky na bezpečnost

Zadavatel požaduje splnění následujících požadavků na bezpečnost:

- Podpora zabezpečení sítě - Infrastruktura musí být koncipována tak, aby síťová komunikace využívala výhradně protokolu TCP, přičemž na straně komponenty poskytující služby (server) využívala statických, předem známých portů. Protokol UDP lze použít pouze pro komunikaci v rámci DDC a předem definovaných VLAN. Volitelně musí umožnit použití šifrované komunikace.
  Správa účtů administrátora - Účty budou uloženy a spravovány v Microsoft AD Zadavatele.

- Přístup - Přístupy k síťové Infrastruktuře jsou jednotné bez ohledu na to, jestli přistupuje uživatel pomocí uživatelského rozhraní nebo aplikace pomocí webové služby. Vždy je nezbytné provést ověření uživatele a jeho oprávnění přístupu k datům na základě role nebo oprávnění a provést auditní záznam o tomto přístupu (ev. zamítnutí přístupu) a činnosti. Každý přístup musí být jednoznačně identifikován a přiřazen ke uživateli VPN a správci, který s daty pracuje (i v případě přístupu přes API je nutné přebírat identitu uživatele a ověřovat oprávnění).

- Audit - Infrastruktura musí o sobě poskytovat informace důležité pro audit prováděných činností. Každá činnost každého administrátora musí být evidována, součástí evidence je minimálně operace, identita uživatele a čas. Uchazeč bude formou Konzultací rovněž součinit při auditu činnosti koncových uživatelů. Součástí projektu je zpracování návrhu auditního procesu a na jeho základě zapnutí auditního logování pro všechny implementované prvky.

- Monitoring - Infrastruktura musí o sobě poskytovat informace důležité pro provozní a bezpečnostní monitoring. Musí tedy mimo jiné logovat veškeré operace ohledně

přístupu a oprávnění administrátorů, a to jak úspěšné, tak neúspěšné pokusy o přístup.

- Zálohování - Záloha Infrastruktury musí být integrována do zálohovacího prostředí Zadavatele. Zálohovací systém bude zálohovat jak data, tak celé virtuální servery.

3.11 Požadavky na spolupráci s provozovateli systémů/aplikací

Vlastní implementaci nových systémů JISPSV, migraci stávajících aplikací nebo dat bude zajišťovat provozovatel daného systému/aplikace, pravděpodobně v několika fázích.

V průběhu migrace systémů/aplikací Uchazeč poskytne provozovatelům aplikací všechny požadované informace o Infrastruktuře a bude s provozovateli systémů/aplikací spolupracovat na přípravě detailních migračních postupů, podle kterých budou jednotlivé systémy/aplikace migrovány do nového prostředí. Tuto spolupráci bude Uchazeč zajišťovat formou Konzultací řádně schválených Zadavatelem.

Požadované činnosti bude uchazeč realizovat zejména v oblastech:

- spolupráce při migraci dat,
- začlenění aplikací do clusterů,
- implementace dopadů změn operačních systémů,
- vytváření virtuálních strojů dle změnových požadavků provozovatelů systémů/aplikací.

3.12 Požadavky na spolupráci s poskytovatelem služeb podpory provozu současných datových center

Zadavatel přepokládá souběžný provoz stávajích a nových Datových center po dobu několika let. Stávající datová centra jsou spravována jiným dodavatelem. Zadavatel požaduje, aby uchazeč poskytl součinnost a spolupráci při:

- optimalizaci komunikace mezi stávajícími datovými centry a DDC,
- migrací systémů a aplikací mezi stávajícími datovými centry a DDC.

Tuto spolupráci bude Uchazeč zajišťovat formou Konzultací řádně schválených Zadavatelem.

3.13 Požadavky na Služby – Katalog služeb

3.13.1 Definice pojmů

3.13.1.1 Incident

Událost při využívání služby, která neprobíhá očekávaným způsobem a způsobuje, či může způsobit snížení kvality služby nebo její nedostupnost (např. výpadek, případně výrazné zpomalení Infrastruktury, na základě HW poruchy nebo SW chyby vzniklá nedostupnost dat, nedostupnost komunikací, atp.). Incidentem je i jakýkoliv zjištěný bezpečnostní problém i v případě, že neohrožuje okamžitě dostupnost a kvalitu služby.

3.13.1.2 Vada

Vada je příčina, která způsobila incident. Je jí tedy např. SW chyba nebo HW porucha, a to jak vlastní Infrastruktury, tak i systémů podpůrných.

3.13.1.3 Požadavek (request)

Žádost ze strany uživatele služby o zabezpečení podpory při využívání služby předaná na kontaktní místo, která nemá příčinu v chybovém stavu služby, tj. není incidentem (např. žádost o práce, materiál nebo informace poskytované Uchazečem ke službě).

3.13.1.4 Dostupnost

Skutečnost, že Infrastruktura (nebo její definovaná část) je přístupná v požadované kvalitě ve sjednanou dobu a požadovaným způsobem – udává se jako procento skutečného času běhu Infrastruktury z celkové požadované doby běhu Infrastruktury (nebo její definované části).

Infrastruktura (nebo její definovaná část) je označena jako nedostupná v případě nedostupnosti Infrastruktura jako celku nebo podstatné dílčí části této Infrastruktura.

Za nedostupnou se považuje od okamžiku nahlášení Zadavatelem nebo zjištění Uchazeče do okamžiku obnovení plné dostupnosti. Dostupnost je vztažena ke kalendářnímu měsíci. Pro výpočet doby nedostupnosti jsou časy zaokrouhleny na celé minuty. Do doby nedostupnosti se započítávají všechny doby incidentů kategorie A a neplánovaných odstávek. Pokud byl incident způsoben prokazatelně třetí stranou, do doby nedostupnosti se nezapočítává.

3.13.1.5 Provozní doba

Časový úsek, ve kterém je zajištěn provoz a služba je v definovaném rozsahu a kvalitě dostupná uživatelům. Doba provozu zahrnuje dobu podpory, příp. dobu, ve které služba není podporována. Doba provozu je dále členěna na:

- Režim služby / komponenty – Označuje dny v týdnu a hodiny ve dni, kdy je služba/komponenta služby poskytována. Např. 7x24 znamená pracovní i nepracovní dny 24 hodin denně; 5x12 znamená pracovní dny 12 hodin denně (např. 6:00-18:00).
- Zaručená doba provozu (*ZDP*) – Doba, kdy je Uchazeč povinen garantovat dostupnost služby. Tato doba se zahrnuje do výpočtu ukazatelů dostupnosti (QD) a reakce (QR) na incidenty.
- Servisní okno údržby – Doba, kdy je Uchazeč oprávněn provádět plánované servisní zásahy na Infrastruktuře.
- Doba provozu komponenty – Doba, kdy jsou poskytovány činnosti, které jsou náplní dané komponenty služby.

3.13.1.6 Doba podpory

Časový úsek, ve kterém je poskytována uživatelská podpora a zajištěna podpora funkčnosti Infrastruktury. Doba podpory může být rozdělena do časových pásem s definovanou úrovní podpory.

3.13.1.7 Reakční doba na incident/požadavek

Maximální doba, která uplyne od okamžiku nahlášení incidentu/požadavku uživatelem na Service Desk a okamžikem zahájení jeho řešení. Incidenty, které nebudou řešeny řešitelem první úrovně (operátor Service Desku), musí být v této době předány skupině řešitelů vyšší úrovně. Sjednaná hodnota parametru se definuje v popisu služby nebo komponentu služby.

Reakční doba jeden kalendářní den znamená dobu odezvy do 24 hodin včetně mimopracovních hodin od okamžiku nahlášení incidentu na Service Desk Zadavatele. **Reakční doba jedna hodina** znamená dobu 60 minut do zahájení řešení, nebo předání k řešení od okamžiku nahlášení incidentu na Service Desk Zadavatele.

3.13.1.8 Doba vyřešení incidentu/požadavku

Max. doba, která uplyne od okamžiku nahlášení incidentu/požadavku na Service Desk do okamžiku nastavení požadovaného stavu řešitelem a oznámení ukončení řešení uživateli. V případě, že uživatel není s řešením spokojen, znovu se otevírá incident k novému řešení.

Doba řešení nemusí být dodržena v případě:

- že se jedná o známé chyby a nedodělky, které byly známy při předání projektu a dosud nebyly vyřešeny,
- chyby, které mají příčinu v chybné činnosti uživatele (např. spouštění výpočtů v esprávných termínech), pokud tato příčina není způsobena chybou v Infrastruktuře,
- uchazeč dočasným řešením minimalizoval dopad incidentu – převedl na jinou kategorii. Incident se však v takovém případě nepovažuje za vyřešený, pouze se mění spolu se změnou kategorie i doba na vyřešení.

3.13.1.9 NBD

Podporou v rozsahu NBD (Next Business Day) provádí Uchazeč odstranění Vady Infrastruktury a uvedení do bezvadného stavu v místě instalované Infrastruktury, vždy nejpozději do následujícího pracovního dne do 17:00 hod. od vzniku Ticketu v Service Desku.

3.13.1.10 Ticket

Záznam evidovaný v Service Desku Zadavatele. Záznam vznikl na základě požadavku oprávněné osoby nebo na základě automatického hlášení Incidentu dohledovým systémem Uchazeče nebo Zadavatele.

3.13.1.11 Dílčí měsíční výkaz kvality plnění

Sada výkazů sestavovaných Uchazečem na základě informací v Service Desku. Součástí výkazů je provedení vyhodnocení poskytovaných služeb a plnění kvalitativních parametrů. Detailní struktury dílčích reporty budou definovány před zahájením provozu.

3.13.1.12 Souhrnný měsíční výkaz kvality plnění

Výkaz sestavený Uchazečem z dílčích měsíčních výkazů kvality plnění. Výkaz je předložen Zadavateli k odsouhlasení a podepsán oběma smluvními stranami. Podepsaný souhrnný výkaz slouží jako souhlas k uplatnění slevy za služby. Výkaz je předkládán jako příloha k faktuře.

3.13.1.13 MD

Jedná se o jednotku kapacity, která definuje vynaloženou práci jednoho pracovníka za jeden pracovní den, který je tvořen 8 hodinami (jinak rovněž „člověkoden“). Pokud není stanoveno jinak, je požadováno vykazování prováděných činnosti v minutách.

3.13.1.14 Úroveň podpory L1, L2,L3

- L1 úroveň podpory = pracoviště Service Desk Zadavatele zabezpečuje příjem resp. vstupní zpracování všech incidentů, požadavků, jejich prvotní kontrolu a předání řešitelům od autorizovaných interních uživatelů (tj. pracovníků Zadavatele nebo Zadavatelem zmocněných osob) a dodavatelů souvisejících IT komponent. Pozn.: první úroveň podpory pro externí uživatele (tj. např. žadatele, atp.) bude zajišťována Zadavatelem.
- L2 úroveň podpory = označuje první vrstvu řešitelů Uchazeče přijatého požadavku, incidentu.
- L3 úroveň podpory = označuje druhou vrstvu řešitelů Uchazeče, kteří provádějí vysoce specializované činnosti, např. metodicko-technické analýzy složitých problémů.

Všechny záznamy procházející úrovněmi L1 až L3 budou vedeny v systému Service Desk Zadavatele. Řešitelé mohou být jak na straně Uchazeče, tak na straně dodavatelů souvisejících IT komponent příp. řešitelských týmů Zadavatele.

3.13.1.15 Service Desk

Aplikace zpravidla využívána pro potřeby Service Desku pro evidenci, správu a řízení požadavků a incidentů. Pokud není uvedeno jinak, vztahují se všechna vyjádření k aplikaci Zadavatele. V rámci Service Desku jsou řešeny rovněž požadavky a procesy k řízení realizace změn. Na základě informací v Service Desku Zadavatele se provádí vyhodnocení plnění SLA.

3.13.1.16 Kontaktní místo Uchazeče

Pracoviště Uchazeče zajišťující kontakt uživatele na funkci podpora uživatele. Je definované zejména intranetovou adresou SW aplikace a telefonním číslem, příp. emailovou adresou. Kontaktní místo uchazeče však slouží pouze jako záložní komunikační kanál v případě nefunkčnosti Service Desku Zadavatele nebo jako první eskalační úroveň.

3.13.1.17 WF (Workflow)

Workflow označuje pracovní postup, který je definován jednotlivými aktivitami a stavy.

3.13.2 Definice služeb, komponent a částí

Katalog služeb specifikuje služby Uchazeče a činnosti (tzv. komponenty služeb), které vykonává v rámci jednotlivých služeb.

Katalog služeb obsahuje základní minimální výčet parametrů jednotlivých služeb. Předpokládá se, že katalog služeb bude dále rozpracováván v rámci implementačních fází projektu, kde budou rovněž detailně specifikovány související procesy řízení a poskytování služeb.

Služba	Komponenta	Režim
S1 Provozní podpora	KS1.1 Podpora provozu	Paušál
	KS1.2 Uživatelská podpora	Paušál
	KS1.3 Technická a metodická podpora	Paušál
	KS1.4 Bezpečnostní dohled	Paušál
	KS1.5 Technologický update	Paušál
	KS1.6 Záloha a obnova	Paušál
	KS1.7 Dohled nad provozem	Paušál
S2 Vzdělávání administrátorů a správců		Paušál

3.13.2.1 Služba „S1_Provozní podpora“

3.13.2.1.1 Vymezení služby

Označení	Název služby
S1	**Provozní podpora**
Stručný popis služby	
Služba zajišťuje provoz všech logických částí poskytnutého plnění. Její součástí jsou především podpora základních funkcí. Součástí služby je příjem, zpracování a řešení incidentů v úrovni L2 a L3 v systému Service Desk Zadavatele.	
Podmínky poskytování služby	
Předmětem služby je zajištění korektní funkčnosti všech logických částí pro uživatele Infrastruktury, a to v rozsahu akceptované specifikace vytvořené v rámci instalace a implementace a dílčích specifikací, jež jsou výstupem implementovaných změn. Předmětem služby je rovněž zajištění všech náležitostí pro korektní průběh integračních vazeb na jiné systémy v rozsahu akceptované specifikace. Uchazeč bude vykonávat všechny činnosti vedoucí k bezproblémovému chodu všech logických částí ve všech požadovaných prostředí. Činnosti, které zadavatel explicitně požaduje, jsou uvedeny u jednotlivých komponent služby. Zadavatel požaduje plnou funkčnost Infrastruktury na prostředí. Součástí služby jsou všechny činnosti nutné k zajištění požadované dostupnosti a odezvy služby. Zadavatel požaduje plnění například, nikoliv však výlučně, činností uvedených u komponent služby KS1.1 – KS1.7 v rozsahu pokrývající všechny uvedené logické části. Uchazeč zajistí příjem, analýzu, zpracování a řízení incidentů zadaných do Service Desku Zadavatele spadajících do kompetence Uchazeče.	
Seznam komponent služby (oblasti zajišťovaných činností, jejichž detailní popis je uvedeny níže):	
Označení	**Název**
KS1.1	Podpora provozu
KS1.2	Uživatelská podpora
KS1.3	Technická a metodická podpora
KS1.4	Bezpečnostní dohled

KS1.5	Technologický update
KS1.6	Záloha a obnova
KS1.7	Dohled nad provozem
Parametry služby	
Provozní parametry jsou uvedeny u jednotlivých komponent služby.	

3.13.2.1.2 Vymezení komponent služby (zajišťovaných činností)

3.13.2.1.2.1 Komponenta služby „KS1.1 Podpora provozu “

Označení	Název komponenty
KS1.1	**Podpora provozu**
Seznam činností	
Řešení Incidentů	„Řešení Incidentů“ se vztahuje na realizaci všech dílčích činností, které jsou nezbytné pro odstranění dané chyby. Jedná se například, nikoliv však výlučně, o činnosti související s příjmem a analýzou incidentů, návrhu řešení nebo dočasného řešení, realizací oprav a dohledem nad průběhem řešením. Řešení Incidentů se vztahuje na všechny technologické části dané logické části. Opravy chyb se vztahují i na HW a SW třetích stran, který je nedílnou součástí plnění.
Optimalizace chodu	“Optimalizace chodu” zahrnuje dílčí činnosti související s úpravami Infrastruktury (indexace, změny konfigurací, apod.) s cílem udržet požadované výkonnostní parametry dané logické části. Optimalizace chodu se vztahuje na všechny technologické části dané logické části a zahrnuje také optimalizaci provozu z hlediska požadavků na zdroje
Kontrola logů	„Kontrola logů“ zajišťuje všechny dílčí činnosti spojené s proaktivní kontrolou chodu logické části s cílem včas odhalit potenciální problémy související s provozem Infrastruktury. O provedení kontroly logů bude vždy proveden záznam do Service Desku tak, aby bylo možné vyhodnotit kvalitu poskytované služby. Součástí záznamu v Service Desk bude i informace o potencionálních problémech, které byly v rámci logů identifikovány. Zálohování logů bude prováděno v rámci činnosti zálohování.
Zvýšená provozní podpora	„Zvýšená provozní podpora“ zahrnuje činnosti související se změnou parametrů nutných pro provoz Infrastruktury, které si nebude Zadavatel vykonávat sám prostřednictvím vlastních pracovníků. Jedná se o činnosti související s realizací změn, podporou a poskytování součinnosti při nasazování, testování změn komponent jiných dodavatelů, jejichž provoz má úzkou souvislost s provozem a účast pracovníků Uchazeče na pravidelných poradách. Činnosti a jejich náročnosti bude Uchazeč vykazovat v granularitě 0,25 MD a budou samostatně uvedeny v měsíčním reportu. Činnosti budou realizovány až na základě schválení oprávněnou osobou Zadavatele.

Správa prostředí	"Správa prostředí" zahrnuje dílčí činnosti související se správou prostředí a všech jeho vrstev. Uchazeč vykonává sám prostřednictvím vlastních pracovníků. Uchazeč tuto činnost vykonává na všech požadovaných prostředích Zadavatele. Prostředí zadavatele tvoří následující vrstvy: 1. technologická vrstva HW, 2. virtualizační vrstva, 3. vrstva pro ukládání dat, 4. komunikační vrstva, 5. dohledová a monitorovací vrstva. Nedílnou součástí je průběžná aktualizace provozní dokumentace.

Podmínky provádění činností

Zadavatel požaduje provádění všech výše definovaných činností v takovém rozsahu, aby byla zachována požadovaná dostupnost Infrastruktury a všech jejích logických částí. V případě, že provádění činností vyžaduje odstávku logické části, je uchazeč povinen navrhnout provedení dané činnosti a provést ji po odsouhlasení Zadavatelem pouze v předem stanoveném servisním okně a podle procesu Proces plánovaných zásahů. Toto servisní okno bude maximálně v rozsahu 4 hodin měsíčně. Pravidelnost plánování servisního okna včetně seznamu všech pravidelných úkonů bude stanovena v úvodní fázi, kde bude Proces plánovaných zásahů Uchazečem představen.
Zadavatel požaduje vedení podrobné provozní dokumentace o rozsahu pravidelných i nepravidelných prací s uvedením jména nebo kódu pracovníka, který činnosti prováděl a časovým razítkem. Provozní dokumentace bude vedena na centrálním úložišti Zadavatele v dostatečném rozsahu pro potřeby vyhodnocení kvality služby.
Uchazeč je povinen zaznamenat každý realizovaný výkon včetně podrobné informace do Service Desku nejpozději do 2 hodin od jejího výskytu a průběžně aktualizovat její stav vzhledem k jejímu vývoji.

Obsah plnění

Rozsah plnění ze strany Uchazeče bude zahrnovat:

a) Veškeré licenční poplatky spojené s údržbou technologií a komponent, které byly Uchazečem použity pro realizaci nabízeného řešení dle licenční politiky příslušných výrobců/dodavatelů.
b) Náklady na pracovníky Uchazeče, kteří budou zajišťovat požadované činnosti.
c) Veškeré náklady související se zajištěním definovaných činností.

Rozsah činností

Zadavatel požaduje následující rozsah činností:

Řešení Incidentů	Řešení Incidentů je dáno aktuální potřebou. Činnosti budou realizovány bez časového, věcného a množstevního omezení.
Optimalizace chodu	Úpravy Infrastruktury jsou dány aktuální potřebou a budou realizovány bez časového, věcného a množstevního omezení.
Kontrola logů	Kontrola logů v minimálním rozsahu 1x za den jako prevence proti výpadkům.
Zvýšená provozní podpora	Zadavatel předpokládá využití v rozsahu maximálně 4 MD měsíčně. Nevyčerpaná část bude převoditelná do dalšího období.
Správa prostředí	Činnosti budou realizovány bez časového, věcného a množstevního omezení.

„Podpora provozu" bude Uchazečem zajišťována jako paušální plnění, což znamená, že Uchazeč bude zajišťovat potřebné činnosti v takovém rozsahu, který bude nezbytný pro dosažení všech kvalitativních parametrů příslušné služby.

Provozní doba poskytování komponenty		
Komponenta “Podpora provozu” bude poskytována v režimu 7x24 (Po-Ne, 00:00 – 24:00 hod) včetně státních svátků a dnů pracovního volna.		
Reakční lhůty pro poskytování služby		
Typ požadavku	Reakční doba v hodinách	Doba vyřešení v hodinách
Požadavek uživatele	2	Dle dohody, maximálně však do 10 kalendářních dnů.
Incident	Dle požadavku v kap. 3.13.1.7	Dle požadavku v kap. 3.13.1.8
Reakční lhůta běží v provozní dobu poskytování komponenty a začíná od okamžiku zapsání požadavku oprávněnou osobou do Service Desku. Reakční lhůta na vyřešení požadavku se vztahuje na všechny činnosti nutné pro vyřešení požadavku v prostředí, pokud Zadavatel v daném případě nestanovil jinak.		

3.13.2.1.2.2 Komponenta služby „KS1.2 Uživatelská podpora“

Označení	Název komponenty
KS1.2	**Uživatelská podpora**
Seznam činností	
Řešení požadavků uživatelů (administrátorů a správců)	„Řešení požadavků uživatelů“ se vztahuje na realizaci všech dílčích činností, které jsou nezbytné pro vyřešení požadavků správců a adminstrátorů. Jedná se například, nikoliv však výlučně, o činnosti související s přijetím, analýzou a řešením požadavků na úrovni L2.
Zvýšená uživatelská podpora	„Zvýšená uživatelská podpora“ zahrnuje činnosti související s úpravou parametrů nebo úpravou kritických konfigurací Infrastruktury, které si nebude Zadavatel vykonávat sám prostřednictvím vlastních pracovníků. Jedná se o činnosti související s realizací drobných úprav na základě požadavků oprávněných osob Zadavatele. Činnosti a jejich náročnosti bude Uchazeč vykazovat v granularitě 0,25 MD a budou samostatně uvedeny v měsíčním reportu.
Podmínky provádění činností	
Zadavatel požaduje provádění všech výše definovaných činností v takovém rozsahu, aby byla zachována požadovaná dostupnost dané logické části. Uchazeč je povinen zaznamenat každý realizovaný výkon včetně podrobné informace do Service Desku nejpozději do 2 hodin od jejího výskytu a průběžně aktualizovat její stav vzhledem k jejímu vývoji.	
Obsah plnění	
Rozsah plnění ze strany Uchazeče bude zahrnovat: a) Veškeré licenční poplatky spojené s údržbou technologií a komponent, které byly uchazečem použity pro realizaci nabízeného řešení dle licenční politiky příslušných výrobců/dodavatelů. b) Náklady na pracovníky Uchazeče, kteří budou zajišťovat požadované činnosti. c) Ostatní náklady související se zajištěním definovaných činností.	

Rozsah činností	
Zadavatel požaduje následující rozsah činností:	
Řešení požadavků uživatelů	Příjem a analýza požadavků a řešení incidentů jsou dány aktuální potřebou a budou realizovány bez časového, věcného a množstevního omezení.
Zvýšená uživatelská podpora	Zadavatel předpokládá využití v rozsahu maximálně 2 MD měsíčně. Nevyčerpaná část bude převoditelná do dalšího období.
„Uživatelská podpora“ bude Uchazečem zajišťována jako paušální plnění, což znamená, že Uchazeč bude zajišťovat potřebné činnosti v takovém rozsahu, který bude nezbytný pro dosažení všech kvalitativních parametrů příslušné služby.	
Provozní doba poskytování komponenty	
Komponenta “Uživatelská podpora” bude poskytována v režimu 5x12 (Po-Pá, 06:00 – 18:00 hod, pracovní dny vyjma svátků).	
Reakční lhůty pro poskytování služby	

Typ požadavku	Reakční doba v hodinách	Doba vyřešení v hodinách
Požadavek uživatele	2	Dle dohody, maximálně však do 10 kalendářních dnů.

Reakční lhůta běží v provozní dobu poskytování komponenty a začíná od okamžiku zapsání požadavku oprávněnou osobou do Service Desku. Reakční lhůta na vyřešení požadavku se vztahuje na všechny činnosti nutné pro vyřešení požadavku v prostředí, pokud Zadavatel v daném případě nestanovil jinak.

3.13.2.1.2.3 Komponenta služby „KS1.3 Technická a metodická podpora “

Označení	Název komponenty
KS1.3	**Technická a metodická podpora**
Seznam činností	
Provozní konzultace	„Provozní konzultace“ zahrnuje činnosti související s poradenstvím provozních činností příslušné logické části. Jedná se zejména o konzultace v oblasti administrace, správy Infrastruktury, nastavení práv, audity, zálohování, obnova apod.
Organizační konzultace	„Organizační konzultace“ zahrnuje činnosti související s organizační stránkou zajištění dodávky služby a provozu. Jedná se zejména, nikoliv však výlučně, o účast Uchazeče na pracovních jednáních, seminářích, prezentacích, zpracování výkazů, poskytnutí součinnosti pro certifikaci atd.
Analytická konzultace	„Analytická konzultace“ zahrnuje činnosti související s rozvojem funkcionality příslušné logické části. Jedná se např. o činnosti zpracování návrhu, oponentura záměrů, poradenství v oblasti fungování dané logické části, konzultace k provozu agendových IS, hodnocení výkonnosti a výkazy kapacitního využití diskových polí atd.
Metodická konzultace	„Metodická konzultace zahrnuje činnosti související s metodickou stránkou fungování příslušné logické části. Jedná se tedy o IT konzultace v oblasti metodiky monitorování, ITILu a konzultace

	k práci s Infrastrukturou ve vztahu k problematice metodik Zadavatele.
Ostatní provozní konzultace	„Ostatní provozní konzultace“ zahrnují činnosti spojené s poskytování součinnosti k přípravě, testování, realizaci změn Infrastruktury. Jedná se o konzultace odborných specialistů v rozsahu použitých technologií. Činnosti a jejich náročnosti bude Uchazeč vykazovat v granularitě 0,25 MD a budou samostatně uvedeny v měsíčním reportu. Činnosti budou realizovány až a základě schválení oprávněnou osobou Zadavatele.

Podmínky provádění činností

V rámci technické a metodické podpory zajistí Uchazeč pro pověřené pracovníky Zadavatele (administrátoři, správci) konzultace související s provozem a rozvojem příslušné logické části na L2 a L3 úrovni. Komunikace bude probíhat prioritně ve stanovených projektových týmech. Jako komunikační kanál bude zvolen email, telefon nebo videokonference v rámci kontaktů uvedených v projektových týmech, nebo Uchazeč zajistí příslušný kontakt v případě přesahu tématu do jiné tematické oblasti.
Zadavatel i Uchazeč jsou povinni zaznamenávat všechny požadavky na konzultace do Service Desku tak, aby bylo možné vyhodnotit jednotlivé parametry hodnocení služeb. Uchazeč je povinen zaznamenat (a to i v případě konzultace po telefonu) příslušnou informaci do Service Desku nejpozději do 2 hodin od jejího výskytu a průběžně aktualizovat její stav vzhledem k jejímu vývoji.
Granularita vykazování komponenty je 0,25 MD.

Obsah plnění

Rozsah plnění ze strany Uchazeče bude zahrnovat:

a) Náklady na technické a materiální vybavení související s poskytováním konzultací včetně licenčních nákladů na autorská díla, pokud jsou tyto díla nezbytná pro poskytování dané konzultace.
b) Personální náklady na pracovníky Uchazeče, kteří budou zajišťovat požadované činnosti.
c) Dopravní a cestovní náklady související s přepravou pracovníků Uchazeče do místa konzultace.

Rozsah činností

Zadavatel požaduje následující rozsah činností:

Provozní konzultace	Zadavatel předpokládá rozsah 2 MD za 1 kalendářní měsíc.
Organizační konzultace	Zadavatel předpokládá rozsah 0,25 MD za 1 kalendářní měsíc.
Analytická konzultace	Zadavatel předpokládá rozsah 0,5 MD za 1 kalendářní měsíc.
Metodická konzultace	Zadavatel předpokládá rozsah 0,25 MD za 1 kalendářní měsíc.
Ostatní provozní konzultace	Zadavatel předpokládá rozsah 0,25 MD za 1 kalendářní měsíc.

Komponenta „Technická a metodická podpora “ bude Uchazečem zajišťována jako paušální plnění, což znamená, že Uchazeč bude zajišťovat potřebné činnosti v takovém rozsahu, který bude nezbytný pro dosažení všech kvalitativních parametrů příslušné služby. Rozsah plnění ze strany Uchazeče bude omezen požadovaným rozsahem činností. Nevyčerpané MD technické a metodické podpory budou převedeny do dalšího období.

Provozní doba poskytování komponenty		
Komponenta “Technická a metodická podpora” bude poskytována v režimu 5x12 (pracovní dny mimo státní svátky a dny pracovního volna od 6:00 do 18:00).		
Reakční lhůty pro poskytování služby		
Typ požadavku	Reakční doba v hodinách	Doba vyřešení v hodinách
Požadavek uživatele	2	Dle dohody, maximálně však do 10 kalendářních dnů.
Reakční lhůta běží v provozní dobu poskytování komponenty a začíná od okamžiku zapsání požadavku oprávněnou osobou do Service Desku. Reakční lhůta na vyřešení požadavku se vztahuje na všechny činnosti nutné pro vyřešení požadavku v provozním, pokud Zadavatel v daném případě nestanovil jinak.		

3.13.2.1.2.4 Komponenta služby “KS1.4 Bezpečnostní dohled “

Označení	Název komponenty
KS1.4	**Bezpečnostní dohled**
Seznam činností	
Součinnost	Poskytnutí součinnosti pracovníkům Zadavatele, kteří realizují bezpečnostní audit a dohled. Jedná se například o zpřístupnění všech logů, umožnění penetračních testů, zpřístupnění dokumentace a apod.
Zpracování auditní stopy	„Zpracování auditní stopy“ zahrnují dílčí činnosti související s identifikací a rozborem datových informací auditních logů, s cílem interpretovat auditní stopu prováděných činností uživatelů a administrátorů systémů.
Bezpečnostní dohled	Výkon bezpečnostního dohledu a realizace bezpečnostních opatření identifikovaných ve výstupech z bezpečnostních dohledů a auditů na základě pravidel definovaných v úvodní fázi při definici Bezpečnostního projektu. Bezpečnostní dohled se vztahuje na realizaci všech dílčích činností, které jsou nezbytné pro bližší identifikaci bezpečnostního incidentu a návrhu vhodných protiopatření.
Podmínky provádění činností	
Uchazeč je povinen sledovat a upozorňovat na bezpečnostní incidenty identifikované v rámci provozu z pohledu vnější bezpečnosti, vnitřní bezpečnosti i ochraně citlivých a osobních dat. Zadavatel (resp. jím určený subjekt) i Uchazeč jsou povinni zaznamenávat veškeré aktivity (události, incidenty, požadavky, komentáře, atd.) související s komponentou služeb „Bezpečnostní dohled“ do Service Desku tak, aby bylo možné vyhodnotit jednotlivé parametry hodnocení služeb. Uchazeč bude aktualizovat dokumentaci v oblasti bezpečnosti s ohledem na identifikované bezpečností incidenty, jejich nápravě nebo protiopatření k jejich zmírnění. Uchazeč je povinen zaznamenat příslušnou informaci do Service Desku nejpozději do 2 hodin od jejího výskytu a průběžně aktualizovat její stav vzhledem k jejímu vývoji. Mechanizmy automatického vyhodnocování pravidel pro identifikaci možných bezpečnostních rizik budou provozovány v režimu komponenty „KS1.1 Podpora provozu“.	

Obsah plnění
Rozsah plnění ze strany Uchazeče bude zahrnovat: a) Náklady na technické a materiální vybavení související s poskytováním součinnosti a realizaci bezpečnostních opatření. b) Náklady na licenční a servisní poplatky třetím stranám, které vyplývají z nasazení a použití SW třetích stran. c) Personální náklady na pracovníky Uchazeče, kteří budou zajišťovat požadované činnosti. d) Dopravní a cestovní náklady související s přepravou pracovníků Uchazeče do místa konzultace, pokud se toto místo nachází na území ČR.
Rozsah činností
Zadavatel požaduje následující rozsah činností: Součinnost — Poskytnutí součinnosti v rozsahu 2 MD za jeden kalendářní měsíc. Zpracování auditní stopy — Součinnost při zpracování auditní stopy v min. rozsahu 40 auditních stop za 1 kalendářní měsíc Bezpečnostní dohled — Realizace bez časového, věcného a množstevního omezení. Komponenta "Bezpečnostní dohled" bude Uchazečem zajišťována jako paušální plnění, což znamená, že Uchazeč bude zajišťovat potřebné činnosti v takovém rozsahu, který bude nezbytný pro dosažení všech kvalitativních parametrů příslušné služby. Rozsah plnění ze strany Uchazeče bude omezen požadovaným rozsahem činností. Činnosti a jejich náročnosti bude Uchazeč vykazovat v granularitě 0,25 MD a budou samostatně uvedeny v měsíčním reportu. Nevyčerpané MD budou převedeny do dalšího období.
Provozní doba poskytování komponenty
Komponenta "Bezpečnostní dohled" bude poskytována v režimu 5x12 (pracovní dny mimo státní svátky a dny pracovního volna od 6:00 do 18:00).

Reakční lhůty pro poskytování služby		
Typ požadavku	Reakční doba v hodinách	Doba vyřešení v hodinách
Požadavek uživatele	2	Dle dohody, maximálně však do 14 kalendářních dnů.
Reakční lhůta běží v provozní dobu poskytování komponenty a začíná od okamžiku zapsání požadavku oprávněnou osobou do Service Desku. Reakční lhůta na vyřešení požadavku se vztahuje na všechny činnosti nutné pro vyřešení požadavku v prostředí, pokud Zadavatel v daném případě nestanovil jinak.		

3.13.2.1.2.5 Komponenta služby "KS1.5 Technologický update"

Označení	Název komponenty
KS1.5	**Technologický update**
Seznam činností	
Monitoring	V rámci monitoringu musí Uchazeč neustále sledovat nové verze systémového SW tak, aby postupnou implementaci těchto nových verzí byly logické části provozovány v aktuálních verzích po celou dobu servisního kontraktu.

Součinnost	V rámci poskytování součinnosti zajistí Uchazeč vzájemnou spolupráci (komunikaci, poskytování informací, účast na jednáních, atd.) s provozovatelem agendových IS a provozovatelem NON-IT infrastruktury serverovny k dosažení a udržení vzájemné vnitřní kompatibility celé Infrastruktury a dále „vnější“ kompatibility s programovým vybavením Zadavatele.
Technologický update	Realizace technologických opatření (testování a instalace oprav systémových SW provozovaných Uchazečem pro podporu provozu) vyplývající z monitoringu a poskytované součinnosti. Technologický update se na vyžádání Zadavatelem vztahuje na realizaci všech dílčích činností, které jsou nezbytné pro odstranění technologické nekonzistentnosti. Technologický update se vztahuje i na SW třetích stran, který je nedílnou součástí dané logické části.
Zvýšená podpora pro technologický update	Činnosti nad rámec „Technologického update“. Jedná se zejména o poskytnutí součinnosti při realizaci změn pro instalace nových verzí systémového SW ve správě Uchazeče. Činnost bude realizována až na základě schválení oprávněnou osobou Zadavatele. Činnosti a jejich náročnosti bude Uchazeč vykazovat v granularitě 0,25 MD a budou samostatně uvedeny v měsíčním reportu.

Podmínky provádění činností

Zadavatel i Uchazeč jsou povinni zaznamenávat veškeré aktivity (události, incidenty, požadavky, komentáře, atd.) související s komponentou služeb „Technologický update“ do Service Desk Zadavatele. Uchazeč je povinen zaznamenat příslušnou informaci do Service Desku nejpozději do 2 hodin od jejího výskytu a průběžně aktualizovat její stav vzhledem k jejímu vývoji.
Realizaci technologického updatu jakékoliv logické části bude schvalovat odpovědný pracovník Zadavatele na základě návrhu Uchazeče. Každý návrh bude obsahovat výčet činností a možných dopadů na okolní systémy.
Kontrolu prováděných akcí bude provádět Zadavatel nebo třetí strana určená Zadavatelem.
Součástí realizace změn je bezodkladná aktualizace provozní dokumentace .

Obsah plnění

Rozsah plnění ze strany Uchazeče bude zahrnovat:

a) Náklady na technické a materiální vybavení související s poskytováním součinnosti, monitoringu a realizaci technologických opatření.
b) Náklady na licenční a servisní poplatky třetím stranám, které vyplývají z nasazení a použití SW třetích stran.
c) Personální náklady na pracovníky Uchazeče, kteří budou zajišťovat požadované činnosti.
d) Dopravní a cestovní náklady související s přepravou pracovníků Uchazeče do místa konzultace, pokud se toto místo nachází na území ČR.

Rozsah činností

Zadavatel požaduje následující rozsah činností:

Součinnost	Zadavatel předpokládá poskytnutí součinnosti v minimálním rozsahu 10 MD za jeden kalendářní rok.
Monitoring	Průběžný monitoring updatů systémových SW prostředků v minimálním rozsahu 1x měsíčně.
Technologický update	Realizace bez časového, věcného a množstevního omezení.
Zvýšená podpora pro technologický update	Zadavatel předpokládá rozsah 2 MD za 1 kalendářní měsíc.

Komponenta „Technologický update“ bude Uchazečem zajišťována jako paušální plnění, což znamená, že Uchazeč bude zajišťovat potřebné činnosti v takovém rozsahu, který bude nezbytný pro dosažení všech kvalitativních parametrů příslušné služby. Rozsah plnění ze strany Uchazeče bude omezen požadovaným rozsahem činností. Nevyčerpané MD budou převedeny do dalšího období.

Provozní doba poskytování komponenty

Komponenta “Technologický update” bude poskytována v režimu 5x12 (pracovní dny mimo státní svátky a dny pracovního volna od 6:00 do 18:00).

Reakční lhůty pro poskytování služby

Typ požadavku	Reakční doba v hodinách	Doba vyřešení v hodinách
Požadavek uživatele	2	Dle dohody, maximálně však do 10 kalendářních dnů.

Reakční lhůta běží v provozní dobu poskytování komponenty a začíná od okamžiku zapsání požadavku oprávněnou osobou (vč. požadavků, které vzniknou interně v rámci činnosti Uchazeče) do Service Desku . Reakční lhůta na vyřešení požadavku se vztahuje na všechny činnosti nutné pro vyřešení požadavku v prostředí, pokud Zadavatel v daném případě nestanovil jinak.
Reakční lhůty na incidenty jsou stanoveny jednotně pro všechny logické částí a pro všechny služby a komponenty.

3.13.2.1.2.6 Komponenta služby “KS1.6_Záloha a obnova “

Označení	Název komponenty
KS1.6	**Záloha a obnova**
Seznam činností	
Zálohovací plán	Jedná se o průběžnou aktualizaci zálohovacího plánu pro všechny logické části. Součástí komponenty je rovněž aktualizace zpracované dokumentace: Recovery plán, Havarijní plán a plán kontinuity služeb, Analýzu rizik.
Test obnovy	V součinnosti se Zadavatelem zajistí Uchazeč test obnovy spočívající v obnově všech částí vrstev. Test obnovy spočívá v zajištění těchto činnosti: • Obnova dat ze záloh. • Ověření validity dat. • Ověření funkčnosti integrací. • Ověření funkčností.
Kontrola záloh	Jedná se o činnosti související s kontrolou záloh. Vlastní proces zálohování provádí garant zálohování (koordinaci zajistí Zadavatel). Kontrola záloh spočívá v provedení: • Kontroly úplnosti záloh. • Kontroly logů agenta zálohovacího SW. • Kontroly velikosti zálohovaných dat. • Vedení zápisu.

Zvýšená podpora a zálohování obnovy	„Zvýšená podpora zálohování a obnovy“ zahrnují činnosti spojené s poskytování součinnosti k přípravě, testování, realizaci změn zálohovacího systému a jeho rekonfigurací. Součásti služby je rovněž realizace speciálních testů obnovy celé Infrastruktury nebo některých jeho logických částí. Činnosti a jejich náročnosti bude Uchazeč vykazovat v granularitě 0,25 MD a budou samostatně uvedeny v měsíčním reportu. Činnosti budou realizovány až a základě schválení oprávněnou osobou Zadavatele.

Podmínky provádění činností

Zadavatel požaduje, aby Uchazeč vykonával denní kontroly zálohovacích rutin. Jedná se zejména o kontrolu vlastního provedení zálohy, kontrolu integrity a úplnosti záloh, kontrolu příslušných logů zálohovacího SW, velikostí záloh a kontroly dodržování předepsaných postupů. Uchazeč bude mít pasivní práva k monitoringu backupů k zajištění tohoto požadavku, vlastní realizaci záloh provádí Zadavatel. Zadavatel požaduje denní zaznamenání podrobného reportu do aplikace Service Desk s časovým razítkem a jménem / kódem pracovníka, který kontrolu provedl.

Zadavatel požaduje, aby Uchazeč součinil se správcem zálohování, který bude řídit proces úplného Testu Obnovy Infrastruktury i všech uložených dat. Zadavatel zajistí koordinaci a součinnost provozovatelem agendového systemu a provozovatele NON-IT Infrastruktury serverovny.

Test obnovy bude proveden na základě návrhu uchazeče a po odsouhlasení Zadavatelem, do prostředí určeného Zadavatelem. V době Testu Obnovy budou zablokována veškerá přístupová práva tak, aby nemohlo dojít ke zneužití dat ani pouhým zobrazením nepovolané osobě. Po otestování funkcionalit obnovené Infrastruktury budou všechna data z dané instance prokazatelně vymazána.

Všechny kroky Testu Obnovy budou podrobně zapisovány (kdo, co a jak prováděl) s uvedením časových razítek. Souběžně bude provedena kontrola popisu postupů v příručkách, zda rozsahem a úplností vyhovují. Všechny tyto informace budou přehledně, čitelně a srozumitelně uvedeny v protokolu a úplnost protokolu bude podmínkou jeho převzetí Zadavatelem.

Test Obnovy se provádí 1x ročně, maximální doba na předložení finální verze podrobného protokolu Zadavateli je 14 dní od data fyzického provedení. Pokud se stane, že v daném termínu nebude kompletní Test Obnovy úspěšně proveden, bude Uchazečem navržen nejbližší náhradní termín, ve kterém se proces bude opakovat.

Obsah plnění

Rozsah plnění ze strany Uchazeče bude zahrnovat:

a) Náklady na technické a materiální vybavení nezbytné pro zajištění požadovaných činností.
b) Personální náklady na pracovníky Uchazeče, kteří budou zajišťovat požadované činnosti.
c) Dopravní a cestovní náklady související s přepravou pracovníků Uchazeče do místa konzultace, pokud se toto místo nachází na území ČR.

Rozsah činností

Zadavatel požaduje následující rozsah činností:

Příprava a aktualizace zálohovacího plánu	Pro zajištění požadovaných činností požaduje Zadavatel kapacitu v minimálním rozsahu 12 MD za jeden kalendářní rok.
Test obnovy	Zadavatel požaduje realizovat test obnovy v rozsahu 1x za kalendářní rok.
Kontrola záloh	Zadavatel požaduje provádět činnosti kontroly záloh v minimálním rozsahu 1x denně.

Zvýšená podpora zálohování a obnovy.	Zadavatel předpokládá rozsah 2 MD za 1 kalendářní měsíc.
Komponenta služby „Záloha a obnova“ bude Uchazečem zajišťována jako paušální plnění, což znamená, že Uchazeč bude zajišťovat potřebné činnosti v takovém rozsahu, který bude nezbytný pro dosažení všech kvalitativních parametrů příslušné služby. Rozsah plnění ze strany Uchazeče bude omezen požadovaným rozsahem činností. Nevyčerpané MD budou převedeny do dalšího období.	
Provozní doba poskytování komponenty	
Komponenta “Záloha a obnova” bude poskytována v režimu 5x12 (pracovní dny mimo státní svátky a dny pracovního volna od 6:00 do 18:00).	
Reakční lhůty pro poskytování služby	
Typ požadavku	Reakční doba v hodinách / Doba vyřešení v hodinách
Požadavek uživatele	2 / Dle dohody, maximálně však do 10 kalendářních dnů.
Reakční lhůta běží v provozní dobu poskytování komponenty a začíná od okamžiku zapsání požadavku oprávněnou osobou do Service Desku. Reakční lhůta na vyřešení požadavku se vztahuje na všechny činnosti nutné pro vyřešení požadavku v prostředí, pokud Zadavatel v daném případě nestanovil jinak.	

3.13.2.1.2.7 Komponenta služby “KS1.7_Dohled nad provozem“

Označení	Název komponenty
KS1.7	**Dohled nad provozem**
Seznam činností	
Monitoring dostupnosti	Sledování a vyhodnocování kritických parametrů s cílem minimalizovat výpadky z důvodu chyb Infrastruktury.
Monitoring výkonu	Sledování a vyhodnocování výkonnostních parametrů s cílem predikovat budoucí potřeby a chování Infrastruktury.
Monitoring události	Sběr událostí z jednotlivých systémových logů s cílem identifikovat prostřednictvím pokročilých analytických technik potencionální problémy s fungováním.
Návrh a změna parametrů dohledu	Realizace změn nastavení dohledu v úrovni dohledu jednotlivých komponent a nastavení jejich požadovaných parametrů. Zadavatel požaduje, aby Uchazeč na základě pravidelných měsíčních vyhodnocení provozu prováděl aktualizaci návrhu dohledu a předkládal ji Zadavateli před realizací změn ke schválení Zadavateli.
Podmínky provádění činností	
V návaznosti na dohledové a kontrolní činnosti realizované v rámci komponenty „KS1.1 Podpora provozu“ bude Uchazeč vykonávat dohledové činnosti nad provozem celé Infrastruktury. Jedná se o kontinuální automatizovaný dohled jednotlivých relevantních částí Infrastruktury, plně zajišťovaný Uchazečem. Uchazeč umožní Zadavateli přístup k dohledu komponent s úzkou vazbou na např. systémový SW, zálohování, integračních rozhraní atd. V případě zjištění jakékoliv vady / problému v průběhu monitoringu bude Uchazeč	

automaticky generovat tickety do Service Desku Zadavatele, včetně správného rozřazení dle kompetencí.
Zadavatel kromě automatizovaného dohledu parametrů požaduje kontinuální kontroly a analýzy logů, kontroly chování zdrojů a kapacit, kontroly využití a vytížení výkonu. Na základě této pravidelné kontroly Uchazeč vydá konkrétní doporučení Zadavateli v oblasti HW platformy, nebo Infrastruktury serverovny, a to vždy cestou záznamu do Service Desku. V rámci řešení těchto doporučení budou uchovány v Service Desku i konkrétní výsledky komunikace a způsob řešení všech doporučení.
Rozsah monitorovaných dat navrhne Uchazeč a pro potřeby provozu bude odsouhlasen Zadavatelem. V průběhu plnění může být rozsah upravován po odsouhlasení obou smluvních stran. Uchazeč umožní přístup k monitorovacím nástrojům pověřeným osobám Zadavatele a současně zpřístupní Dohled pro automatické vyčítání informací o stavu centrálnímu dohledovému nástroji Zadavatele (Service Desk).

Obsah plnění

Rozsah plnění ze strany Uchazeče bude zahrnovat:

a) Náklady na technické a materiální vybavení nezbytné pro zajištění požadovaných činností.
b) Veškeré poplatky (licence) spojené s užíváním dohledového a monitorovacího SW Uchazeče.
c) Personální náklady na pracovníky Uchazeče, kteří budou zajišťovat požadované činnosti.
d) Dopravní a cestovní náklady související s přepravou pracovníků Uchazeče do místa konzultace, pokud se toto místo nachází na území ČR.

Rozsah činností

Zadavatel požaduje následující rozsah činností:

Monitoring dostupnosti	Zadavatel požaduje zajistit monitorování dostupnosti kritických parametrů v takovém rozsahu, který umožní identifikovat výpadek služeb nejpozději do 5 minut od jeho výskytu. Uchazeč je povinen předat vyhodnocený a v Service Desku zadaný incident (tzn. incident prověřený pracovníkem Uchazeče) příslušnému řešiteli uchazeče nejpozději do 30 minut od jeho výskytu. Informace o incidentu spadajícího do kompetence jiného dodavatele předá zadavateli doplňujícím zápisem do Service Desku nejpozději do 30 minut od jeho výskytu.
Monitoring výkonu	Zadavatel požaduje zajistit monitorování výkonu v takovém rozsahu, který umožní identifikovat výkonnostní problémy nejpozději do 30 minut od jejich výskytu. Uchazeč je povinen předat vyhodnocený a v Service Desku zadaný incident (tzn. incident prověřený pracovníkem Uchazeče) příslušnému řešiteli uchazeče nejpozději do 60 minut od jeho výskytu. Informace o incidentu spadajícího do kompetence jiného dodavatele předá zadavateli doplňujícím zápisem do Service Desku nejpozději do 60 minut od jeho výskytu.
Monitoring události	Zadavatel požaduje zajistit sběr událostí ze systémových služeb takovým způsobem, aby došlo nejpozději do 60 minut od vzniku **relevantní** události (ta, která byla vyhodnocena analytickým aparátem) ke generování odpovídajícího incidentu do Service Desku, který bude směřován na příslušného řešitele. Informace o incidentu spadajícího do kompetence jiného dodavatele předá Zadavateli doplňujícím zápisem do Service Desku nejpozději do 60 minut od jeho výskytu.
Návrh a změna parametrů dohledu	Zadavatel požaduje 4x ročně provést vyhodnocení nastavení dohledového systému a sledovaných parametrů.

Komponenta služby „Dohled nad provozem“ bude Uchazečem zajišťována jako paušální plnění, což znamená, že Uchazeč bude zajišťovat potřebné činnosti v takovém rozsahu, který bude nezbytný pro dosažení všech kvalitativních parametrů příslušné služby. Rozsah plnění ze strany Uchazeče nebude omezen, a to i v takovém případě, pokud množství aktuálně provedených činností bude vyšší, než Zadavatelem deklarovaný minimální rozsah. Uchazeč v rámci součinnosti zpřístupní všechny monitorované body Zadavateli. Rovněž Zadavatel zpřístupní relevantní body pro dohled Uchazeče.

Provozní doba poskytování komponenty

Komponenta “Dohled nad provozem” bude poskytována v režimu 7x24 (Po-Ne, 00:00 – 24:00 hod) včetně státních svátků a dnů pracovního volna.

Reakční lhůty pro poskytování služby

Reakční lhůta běží v provozní dobu poskytování komponenty a začíná od okamžiku zapsání Incidentu do Service Desku. Reakční lhůty na vyřešení Incidentů se vztahují na všechny činnosti nutné k jeho odstranění nebo minimalizaci jeho dopadu (dočasné řešení). Reakční lhůty na incidenty jsou stanoveny jednotně pro všechny logické částí a pro všechny služby a komponenty.

3.13.2.2 Služba „S2_ Vzdělávání administrátorů a správců v době provozu “

3.13.2.2.1 Vymezení služby

Označení	Název služby
S2	**Vzdělávání administrátorů a správců v době provozu**

Stručný popis služby

Služba zajišťuje vzdělávání nových administrátorů a správců, přeškolování existujících na základě požadavku Zadavatele.

Podmínky poskytování služby

Uchazeč zajistí formou presenčních kurzů zaškolení nových pracovníků a přeškolení stávajících pracovníků v rozsahu odpovídajícímu roli uživatelů:

- *Administrátor* (osoba Zadavatele z odboru IT, seznámená detailně s interním fungováním, jeho logických částí, integrací a všemi procesními záležitostmi, které jsou nutné k zajištění bezproblémového chodu Infrastruktury)

Vzdělávání bude určeno zejména pro interní pracovníky Zadavatele.
Uchazeč ke každému kurzu zajistí tištěné a elektronické materiály.
Konkrétní aktivity realizované v rámci služby budou Uchazečem provedeny po dohodě a v úzké součinnosti se Zadavatelem. Zadavatel navrhuje a odsouhlasuje termíny školení a jejich věcnou náplň, přičemž nenaplnění ze strany cílové skupiny není zohledňováno.
Zadavatel předpokládá realizaci ve vlastních prostorech.
Uchazeč zajistí příjem, analýzu, zpracování a řízení požadavků zadaných do Service Desku Zadavatele spadajících do kompetence Uchazeče.

Seznam činností

Příprava školení	Příprava školení zahrnuje činnosti související s přípravou materiálu (tištěných, elektronických), vytvoření plánu školení, obeslání účastníků, zajištění lektora apod.
Realizace školení	Realizace školení zahrnuje činnosti související s pronájmem příslušné výpočetní techniky, účast lektora, zajištění občerstvení, atd.

Obsah plnění

Rozsah plnění ze strany Uchazeče bude zahrnovat:

a) Náklady na licenční poplatky za použití autorský děl, které jsou použity pro účely školení.
b) Personální náklady na pracovníky Uchazeče, kteří budou zajišťovat požadované činnosti.
c) Dopravní a cestovní náklady související s přepravou pracovníků Uchazeče do místa školení, pokud se toto místo nachází na území ČR.
d) Zajištění občerstvení, náklady na pronájem výpočetní techniky.

Rozsah činností

Zadavatel požaduje následující rozsah činností:

a) Zpracování školené problematiky v požadovaném formátu a v dohodnutém rozsahu.
b) Příprava a realizace školení.
c) Školení bude vždy pro maximálně 10 osob, předpokládaný počet školených osob je 20. Konkrétní rozsah délka, způsob realizace kurzů a jejich rozsah (MD) bude stanovena na základě dohody Zadavatele a Uchazeče.
d) Služba bude vykazována na základě skutečně realizovaných a akceptovaných kurzů jako součást měsíčního reportu plnění služeb.
e) Pro zajištění požadovaných činností požaduje zadavatel kapacitu v minimálním rozsahu 5 MD za jeden kalendářní rok. Nevyčerpané MD budou převedeny do dalšího období.

Provozní doba poskytování komponenty

Služba „Vzdělávání adminsitrátorů a správců v době provozu“ bude poskytována v pracovní dny mimo státní svátky a dny pracovního volna od 6:00 do 18:00 pokud se obě strany nedohodnou jinak.

Reakční lhůty pro poskytování služby

Typ požadavku	Reakční doba v hodinách	Doba vyřešení v hodinách
Požadavek uživatele	2	Dle dohody

Reakční lhůta běží v provozní dobu poskytování komponenty a začíná od okamžiku zapsání požadavku oprávněnou osobou (vč. požadavků, které vzniknou interně v rámci činnosti Uchazeče) do Service Desku .

Hodnocení služeb

3.13.2.3 Parametry hodnocení služeb, procentní nastavení

3.13.2.3.1 Parametry Hodnocení služeb

Služba		Komponenta		ZD	SLA Vstupní parametry pro vyhodnocení kvality
S1	Provozní podpora	KS1.1	Podpora provozu	24x7	Incidenty
		KS1.2	Uživatelská podpora	12x5	Požadavky
		KS1.3	Technická a metodická podpora	12x5	Požadavky
		KS1.4	Bezpečnostní dohled	12x5	Požadavky
		KS1.5	Technologický update	12x5	Požadavky
		KS1.6	Záloha a obnova	12x5	Požadavky
		KS1.7	Dohled nad provozem	24x7	Požadavky
S2	Vzdělávání administrátorů a správců v době provozu			-	Dle skutečnosti

Vyhodnocení kvalita poskytovaných služeb bude součástí pravidelných měsíčních reportů. Nedodržení požadovaných SLA parametrů bude zpracováno.

Slevy za nedodržení jednotlivých parametrů se sčítají.

3.13.2.4 Vyhodnocení parametrů plnění dostupnosti

3.13.2.4.1 Výpočet parametru z vykazovaných nedostupností služeb

Parametr	**Dostupnost**
Popis	Dostupností je vyjádřena v % doby, po kterou bude Infrastruktura dostupna. Dostupnost se vyhodnocuje pro zaručenou provozní dobu (ZPD) a mimo ZPD.
Metrika	Dostupnost pro každý prvek se vypočítá dle následujícího vzorce: $A = \frac{(A_{ST} - DT)}{A_{ST}} * 100$ A Dostupnost (Availability) A_{ST} Celková odsouhlasená provozní doba za sledované období (měsíc) bez plánovaných odstávek DT = Celková doba neplánovaných odstávek (výpadků) ve sledovaném období (měsíc).
Metoda	Měření bude prováděno automatickým vyhodnocováním Incidentů (kategorie A) v Service Desku (SD) a porovnáním s informacemi v dohledovém systému.
Časové body	Začátek: Čas evidence nedostupnosti prvku v Service Desku (SD) Konec: Čas nahlášení dostupnosti služby do SD.
Časový interval	Dostupnost bude vypočítávána, hlášena a vyhodnocována měsíčně
Výjimky	Měření bude prováděno pro všechny služby uvedené v KS 1.1 Měření bude prováděno pouze v odsouhlasené provozní době KS 1.1

Dostupnost pro ZPD – Služba KS1.1 Podpora provozu						
Dosažená dostupnost	>99,8%	>99,0%	>97,0%	>95,0%	>90,0%	<90,0%
Sleva z ceny služby	0%	10%	20%	30%	40%	50%
Dostupnost mimo ZPD – Služba KS1.1 Podpora provozu						
Dosažená dostupnost	>98,0%	>94,0%	>90,0%	>86,0%	>80,0%	<80,0%
Sleva z ceny služby	0%	10%	20%	30%	40%	50%

Celková sleva za nedostupnost Infrastruktury je dána součtem slev za nedostupnost v ZPD a mimo ZPD. Do nedostupnosti se nezapočítávají plánovaná servisní okna.

3.13.2.5 Vyhodnocení zpracování incidentů

Vyhodnocení incidentů bude prováděno na základě Kategorie incidentu a prostředí, ve kterém k Incidentu došlo. Do vyhodnocení vstupují parametry Reakční doba a Doba vyřešení.

3.13.2.5.1 Kategorizace Incidentů (vad)

Kategorie A – Vážný incident s nejvyšší prioritou, který má kritický dopad do funkčnosti nebo její logické části a dále incident, který znemožňuje užívání prvků nebo způsobuje vážné provozní problémy.
Kategorie B - Incident, který svým charakterem nespadá do kategorie A. Znamená vážné zhoršení výkonnosti a funkčnosti prvku nebo má zásadní omezení nebo je částečně nefunkční. Jedná se o incidenty odstranitelné, které způsobují problémy při užívání a provozování, ale umožňují provoz. Bezpečnostní incident, který neohrožuje dostupnost služby, spadá vždy do kategorie B.
Kategorie C – Incident, který svým charakterem nespadá do kategorie A nebo kategorie B. Znamená snadno odstranitelné incidenty s minimálním dopadem na funkcionality.

Priority reakce a vyřešení incidentu:
Tabulka níže definuje požadované parametry Reakční doby a požadované doby vyřešení incidentů pro jednotlivé priority.

Priorita	Popis	Reakční doba na incident	Doba vyřešení incidentu
1	Nejvyšší priorita na odstranění chyby	0,5 hodiny	do 4 hodin
2	Vysoká priorita na odstranění chyby	0,5 hodiny	NBD
3	Střední až nízká priorita na odstranění chyby	0,5 hodiny	72 hodin

Incidenty s prioritou 1 a 2 budou řešeny bez ohledu na ZPD.

3.13.2.5.2 Matice přiřazení priorit pro řešení incidentů:

V závislosti na typu a kategorii incidentu je v následující tabulce provedeno přiřazení konkrétní požadované priority. Z vazby na parametry priorit je odvozen požadavek na reakční dobu a požadovanou dobu vyřešení.

Prostředí Zadavatele	Incident Kategorie A	Incident Kategorie B	Incident Kategorie C
Datové centrum A	1	2	3
Datové centrum B	1	2	3

V rámci řešení Incidentu, především vzhledem k požadavku na minimalizaci dopadů Incidentu, může Uchazeč použít i dočasné řešení (náhradní řešení). Dočasné řešení je založené na postupu, jehož pomocí lze nevyhovující stav překlenout či obejít, nebo na úpravě, která eliminuje klíčové negativní dopady Incidentu. Na základě poskytnutí takového dočasného řešení může dojít ke změně klasifikace kategorie Incidentu a tedy i ke snížení Priority. Změnu priority schvaluje Zadavatel.

3.13.2.5.3 Vyhodnocení slevy dle SLA pro Incidenty

Následující tabulka udává výši slevy z ceny Služeb za úhrn překročení Reakční doby jednotlivých kategorií Incidentů. Pro výpočet překročení Reakční doby se nezapočítává tolerance 15 minut u kategorie A a B a tolerance 30 minut u kategorie C, vypočet je prováděn měsíčně.

Kategorie incidentu	Sleva za překročení Reakční doby za každou započatou hodinu	Sleva za překročení Reakční doby za každou započatou hodinu nad **4** násobek požadované Reakční doby dle Priority.
Kategorie A	6000,- Kč	12000,- Kč
Kategorie B	2400,- Kč	4800,- Kč
Kategorie C	600,- Kč	1200,- Kč

Následující tabulka udává výši slevy z ceny Služeb za úhrn překročení Doby vyřešení jednotlivých kategorií Incidentů. Pro výpočet překročení Doby vyřešení se nezapočítává tolerance 15 minut u kategorie A a B a tolerance 30 minut u kategorie C, vypočet je prováděn měsíčně.

Kategorie incidentu	Sleva za překročení požadované Doby vyřešení za každou započatou hodinu	Sleva za překročení Doby vyřešení za každou započatou hodinu nad **4** násobek požadované Doby vyřešení dle Priority.
Kategorie A	18000,- Kč	36000,- Kč
Kategorie B	12000,- Kč	24000,- Kč
Kategorie C	1200,- Kč	2400,- Kč

3.13.2.6 Vyhodnocení zpracování požadavků (requesty)

Následující tabulka udává výši slevy z ceny Služeb za úhrn překročení Reakční doby jednotlivých požadavků. Vypočet je prováděn měsíčně.

Požadavek	Sleva za překročení Reakční doby za každou započatou hodinu	Sleva za překročení Reakční doby za každou započatou hodinu nad **4** násobek požadované Reakční doby dle Priority.
Požadavek	3600,- Kč	7200,- Kč

Následující tabulka udává výši slevy z ceny Služeb za úhrn překročení vyřešení jednotlivých požadavků. Vypočet je prováděn měsíčně.

Požadavek	Sleva za překročení požadované Doby vyřešení za každou započatou hodinu	Sleva za překročení Doby vyřešení za každou započatou hodinu nad **4** násobek požadované Doby vyřešení dle Priority.
Požadavek	9600,- Kč	19200,- Kč

3.13.2.7 Celková kvalita služby

Stanovení slev za poskytování služeb odpovídá kvalitě služeb, tj. odpovídá nedodržení požadovaných parametrů. Jedná se o parametry: dostupnost služeb, dodržování termínů Reakčních dob a dob vyřešení. Jednotlivé dílčí slevy se sčítají.

3.13.2.7.1 Měsíční výkaz kvality plnění dostupnosti

Součástí měsíčního vyhodnocení bude seznam všech dílčích nedostupnosti v ZPD a mimo ZPD a celkový procentuální úhrn za obě tato období.

$$S_N = S_{NZPD} + S_{NOST}$$

S_N Celková sleva za nedostupnost
S_{NZPD} Sleva za nedostupnost v Zaručené provozní době (ZPD)
S_{NOST} Sleva za nedostupnost mimo Zaručenou provozní dobu (ZPD)

3.13.2.7.2 Měsíční výkaz kvality plnění Reakční doby a doby vyřešení

Vyhodnocovány jsou jednotlivé požadavky a incidenty. Celková sleva za nedodržení smluvených termínů je dána součtem slev za překročení jednotlivých případů.

Sleva za nesplnění termínů požadavku

$$S_P = S_{PRD} + S_{PDV}$$

S_P Celková sleva za nedodržení parametrů u požadavků
S_{PRD} Sleva za nedodržení Reakční doby u požadavků
S_{PDV} Sleva za nevyřešení požadavků v dohodnutém termínu. Nedodržení Doby vyřešení.

Sleva za nesplnění termínů Incidentu

$$S_I = S_{IRD} + S_{IDV}$$

S_I Celková sleva za nedodržení parametrů u Incidentů
S_{IRD} Sleva za nedodržení Reakční doby u Incidentů
S_{IDV} Sleva za nevyřešení Incidentů v dohodnutém termínu. Nedodržení Doby vyřešení

Sleva za nesplnění termínů všech případů

$$S_T = \sum S_P + \sum S_I$$

S_T Celková sleva za nedodržení termínů

3.13.2.7.3 Výpočet celkové slevy z poskytovaných služeb

$$S = S_N + S_T$$

S	Celková sleva za vyhodnocovací období
S_N	Celková sleva za nedostupnost
S_T	Celková sleva za nedodržení termínů.

4 POŽADAVKY NA SOUČINNOST ZADAVATELE

Součinnost je seznamem závazků zadavatele za účelem poskytnutí nezbytné podpory v oblastech, které principiálně nemůže sám zajistit uchazeč.

4.1.1 Součinnost zadavatele pro analýzu a návrh

Součinnost pro analýzu a návrh zahrnuje součinnost nezbytnou pro provedení detailní analýzy a detailního návrhu v úvodních fázích projektu.

Zadavatel poskytne pro zpracovování Technického projektu a Bezpečnostního projektu součinnost maximálně 4 odborníků v rozsahu nepřevyšujícím 20% jejich pracovní kapacity. Vzhledem k časovým možnostem odborných pracovníků musí řešitel vycházet z předpokladu, že osobní schůzky mohou být v souladu s časovými možnostmi pracovníků zadavatele realizovány též na libovolných pobočkách či kontaktních pracovištích Úřadu práce v rámci celé České republiky.

Pro potřeby modelování dodávaného řešení poskytne zadavatel centrální model (pro software SparxSystem Enterprise Architect v minimální edici Corporate Edition) přístupný zabezpečeným způsobem přes síť Internet. Přístup k modelu bude poskytován individuálním pracovníkům Uchazeče na základě písemné podepsané žádosti.

Zadavatel tedy požaduje zpracovat a udržovat pro své dokumentační potřeby modely v nástroji SparxSystems Enterprise Architect. Zdali Uchazeč použije pro své potřeby nějaké další nástroje je na jeho rozhodnutí. Pokud však v těchto nástrojích bude zpracovávat výstupy určené pro předání Zadavateli, musí Uchazeč zajistit jejich konverzi.

4.1.2 Součinnost zadavatele pro testování

Součinnost pro testování zahrnuje součinnost nezbytnou pro provedení akceptačních, zátěžových a bezpečnostních testů.

Zadavatel poskytne pro provedení akceptačních testů Uchazečem dle testovacích scénářů připravených Uchazečem a schválených Zadavatelem, součinnost maximálně 4 administrátorů a 4 správců.

Zadavatel zajistí s pomocí vlastních zdrojů či třetí strany návrh a provedení zátěžových (výkonnostních) testů.

Zadavatel zajistí s pomocí vlastních zdrojů či třetí strany provedení bezpečnostních testů Infrastruktury.

4.1.3 Součinnost zadavatele pro nasazení

Součinnost pro nasazení zahrnuje součinnost nezbytnou pro nasazení Infrastruktury do rovozu a při testování.

Zadavatel poskytne pro potřeby provozu Infrastruktury síťovou a komunikační infrastrukturu LAN a WAN. Zajistí tak on-line připojení pracovišť k datovým centrům (centrálním výpočetním střediskům). Zadavatel zajistí součinnost správy sítí pro potřebné změny konfigurací navržené Uchazečem a schválené Zadavatelem.

4.1.4 Součinnost zadavatele pro školení

Součinnost pro školení zahrnuje součinnost nezbytnou pro zajištění služby S2.

Zadavatel zajistí prostory pro provádění školení. Prostory mohou být dislokovány v lokalitách 14 krajských poboček Úřadu práce nebo v lokalitě generálního ředitelství Úřadu práce.

Školící učebny budou svojí velikostí umožňovat školení nejvýše 20 pracovníků. Každá učebna bude vybavena prezentační technikou. Předpokládaný minimální počet účastníků jednoho běhu školení je 10 osob.

4.1.5 Součinnost pro projektové řízení

Součinnost pro projektové řízení zahrnuje součinnost nezbytnou pro realizaci projektu v rovině organizační a řízení projektu.

- Zadavatel zajistí v jednotlivých odůvodnitelných případech Uchazeče v prostorách MPSV, či Generálního ředitelství úřadu práce uzamykatelné kancelář(e) pro omezený počet pracovníků řešitele, včetně umožnění přístupu do budovy.
- Zadavatel zajistí připojení k síti Internet v místě jemu přidělených kanceláří.

5 POUŽITÉ TERMÍNY

Termín	Typ	Význam
AD	Obecné	Active Directory
AJAX	Obecné	Asynchronous Javascript and XML.
AP	Obecné	Agentura práce
API	Informační systémy	Aplikační programový interface
APP	Obecné	Aktivizační pracovní příležitost dle §106 ZoZam
APZ	Obecné	Aktivní Politika Zaměstnanosti
AVMA	Informační technologie	Automatická aktivace virtuálního počítače
BIS	Obecné	Bezpečnostní informační služba
BLOB	Obecné	Binary Large Object
BPMN	Obecné	Business Process Model and Notation
CA	Obecné	Certifikační Autorita
CEDR	Obecné	Centrálním registru dotací provozovaní MFČR
CEF	Obecné	Common Event Format
CIFS	Informační systémy	Common Internet File System
CPU	Obecné	Central Processing Unit (Procesor)
CRL	Informační technologie	Certificate Revocation List - seznam zneplatněných certifikátů.
CSV	Informační technologie	Comma separated value
CÚ	Obecné	Celní úřad
CZ-ISCO	Obecné	Klasifikace zaměstnání dle ČSU
ČR	Obecné	Česká republika
ČSSZ	OVM	Česká správa sociálního zabezpečení
ČSU	OVM	Český statistický úřad (ČSÚ) je ústředním orgánem státní správy České republiky. Byl zřízen dne 8. ledna 1969 zákonem č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy.
DB	Informační systémy	Database
DC	Informační	Datové centrum

Termín	Typ	Význam
	technologie	
DCPM	Informační technologie	Data Center Management Portal
DC SOK nebo Datové centrum A	Informační technologie	Datové centrum Sokolovská
Datové centrum B	Informační technologie	Datové centrum lokalita Praha
DDC	Informační technologie	Společně Datové centrum A a Datové centrum B
DHCP	Informační technologie	Správa adresního prostoru IP protokolu
DMS	Informační systémy	Document Management System
DnB	Dávky	Doplatek na bydlení
DNS	Informační technologie	Domain Name Service
DotInfo	Informační systémy	Systém, který umožňuje vyhledávání nad poskytovateli dotací a návratných finančních výpomocí ze státního rozpočtu ČR. Zprostředkovává zobrazení údajů podle zákona č. 171/2012 Sb.
DS	Informační systémy	Datová schránka, resp. informační systém datových schránek
DWDM	Informační systémy	Vlnový multiplex (WDM) představuje v optických sítích technologii, kterou se při přenosu multiplexuje více optických signálů v jednom optickém vlákně s použitím rozdílných vlnových délek (barev) LED nebo laserů. Je tak umožněno rozšířit kapacitu média nebo provést obousměrnou komunikaci na jednom optickém vlákně.
EHP	Obecné	Evropský hospodářský prostoru
EKIS	Informační systémy	Ekonomický informační systém
ESB	Informační technologie	Enterprise Service Bus
ESF	Obecné	Evropský sociální fond (ESF) je hlavním finančním nástrojem Evropské unie pro podporu zaměstnanosti v členských státech a také pro prosazování hospodářské a sociální soudržnosti.
ESS	Informační systémy	Elektronická spisová služba
EU	Obecné	Evropská unie
Evidence případů	Informační systémy	Registr obsahující aktualizované informace všech zpracovávaných žádostí, jejich stavu i případných rozhodnutí
Evidence subjektů	Informační systémy	Evidence je součástí Modulu podpůrných a průřezových činností
FIM	Informační technologie	Forefront Identity Management
FO	Obecné	Fyzická osoba
FS	Informační systémy	File system - souborový systém je označení pro způsob organizace dat ve formě souborů (a většinou i adresářů) tak, aby k nim bylo možné snadno přistupovat.
FTP	Informační technologie	File Transfer Protocol
FÚ	OVM	Finanční úřad
GP	Obecné	Grantové projekty
GŘ ÚP	Obecné	Generální ředitelství úřadu práce
HTTP	Informační technologie	Hypertext Transfer Protocol
HW	Informační technologie	Hardware
CHM	Obecné	Change management
CHPM	Obecné	Chráněné pracovní místo
IAP	Obecné	Individuální akční plán - metoda práce s klienty na úřadech práce při hledání zaměstnání
ICT	Obecné	Informační a komunikační technologie
IdM	Informační systémy	Identity Management

Termín	Typ	Význam
IMAP		Internet Message Access Protocol) internetový protokol pro vzdálený přístup k e-mailové schránce prostřednictvím e-mailového klienta
IPJIS	Informační systémy	Integrace a Provoz Jednotného Informačního Systému (JIS)
IPPD	Obecné	Integrovaná Podpůrná a Provozní Data
IPPR	Obecné	Individuální plán pracovní rehabilitace
IS	Informační systémy	Informační systém
IS SD	Informační systémy	Informační systém socálních dávek
IS ZAM	Informační systémy	Informační systém Zaměstnanost
ISZR	Informační systémy	Informační systém základních registrů
IT	Informační technologie	Informační technologie
JIP/KAAS	Informační systémy	
JSON	Informační technologie	JavaScript Object Notation
JVM	Informační technologie	Jednotné výplatní místo
KDC	Informační technologie	Kerberos Domen Controler
KI	Obecné	Komunikační technologie
KKOV	Obecné	Klasifikace kódů oborů vzdělání
KoP	Obecné	Kontaktní pracoviště
KrP	Obecné	Krajská pobočka
KÚ	Obecné	Krajský úřad
LAN	Informační technologie	Local Area Network (lokální síť)
LPS	OVM	Lékařská posudková služba
MD	Obecné	Jednotka kapacity, která definuje vynaloženou práci jednoho pracovníka za jeden pracovní den
MFČR	OVM	Ministerstvo financí ČR
MK	Obecné	Modrá karta
MMR	OVM	Ministerstvo pro místní rozvoj
MO	OVM	Ministerstvo obrany
MOP	Dávky	Mimořádná okamžitá pomoc
MPSV	OVM	Ministerstvo práce a sociálních věcí
MS	Informační systémy	MicroSoft
MSČR	Obecné	Ministrerstvo spravedlnosti ČR
MŠMT	OVM	Ministerstvo školství, mládeže a tělovýchovy
MV	OVM	Ministerstvo vnitra
MVC	Obecné	Model - View - Controller
MZ	Obecné	Monitorovací zpráva
NB	Informační technologie	Notebook
NBD	Obecné	Následující pracovní den
NIP	Obecné	Národní individuální projekty zaměřené na nástroje a opatření APZ
NPP	Obecné	Příspěvek při přechodu na nový podnikatelský program dle §117 ZoZam
NSP	Obecné	Národní soustava povolání
NTP	Informační technologie	Network Time Protocol
ORM	Informační technologie	Object Relationship Mapping
OS	Informační systémy	Operační Systém
OSSZ	Obecné	Okresní správa sociálního zabezpečení
OSVČ	Obecné	Osoba samostatně výdělečně činná
OUO	Obecné	Oprávněná úřední osoba, vystupuje jako uživatel systému.
OVM	OVM	Orgán veřejné moci
OZP	Obecné	Osoba se zdravotním postižením
PC	Informační technologie	Personal Computer - osobní počítač

Termín	Typ	Význam
PIN	Obecné	Personal Identification Number - osobní ověřovací číslo
PkZ	Obecné	Povolení k zaměstnání
PM	Obecné	Project management
PnP	Dávky	Příspěvek na péči
PnŽ	Dávky	Příspěvek na živobytí
PO	Obecné	Právnická osoba
PP	Obecné	Na Poříčním Právu
PKI	Informační systémy	Public Key Infrastructure
POP3	Informační systémy	Post Office Protocol) internetový protokol, který se používá pro stahování emailových zpráv
Portál	Informační systémy	Webový portál, který obsahuje veřejnou část a část přístupnou po přihlášení. Slouží k publikování informací veřejnosti a vybraným subjektům a ke vstupu (hlašení, formulářů žádostí, atp.) od externích subjektů (klientů, obcí, zaměstnavatelů ato.) směrem k MPSV a ÚP.
Portálu	Informační systémy	Integrovaný portál MPSV
PP	Obecné	Překlenovací příspěvek del §114 ZoZam
PpR	Obecné	Podpora při rekvalifikaci
PR	Obecné	Pracovní rehabilitace
PSS	Obecné	Poskytovatel sociálních služeb
PÚhr	Dávky	Příspěvek na úhradu potřeb dítěte
PvN	Obecné	Podpora v nezaměstnanosti
PZ	Obecné	Příspěvek na zapracování dle §116 ZoZam
RAM	Obecné	Random-access memory
REST	Informační technologie	Representational State Transfer
RDC	Informační technologie	Redesignované datové centrum MPSV
RIP	Obecné	Regionální individuální projekty standardní nástroje a opatření APZ na území jednoho nebo více krajů.
RK	Obecné	Rekvalifikační kurz
ROB	Obecné	Registr obyvatel je součástí Systému základních registrů. Eviduje referenční údaje o FO. Jedná se o občany ČR a EU, cizince s povolením pobytu v ČR a cizince, kterým byla na území ČR udělena mezinárodní ochrana formou azylu nebo doplňkové ochrany. Zdrojem dat jsou současné relevantní evidence.
ROS	Obecné	Základní registr osob je součástí Systému základních registrů. Jeho správcem je ČSU. Eviduje právnické osoby a organizační složky právnických osob, podnikající fyzické osoby, podnikající zahraniční osoby a organizační složky zahraničních osob, organizace s mezinárodním prvkem, organizační složky státu a orgány veřejné moci.
RPSS	Obecné	Registr poskytovatelů sociálních služeb
RTr	Obecné	Rejstříku trestů
RUIAN	Obecné	Registr územní identifikace, adres a nemovitostí
ŘO	Obecné	Řídící orgán
SAN	Informační technologie	Storage area network je dedikovaná (oddělená od LAN, WAN, atd) datová síť
SCCM	Informační systémy	Configuration Management
SCORM	Informační systémy	Shareable Content Object Reference Model (SCORM) je referenční model pro e-learning
SED	Informační systémy	Strukturovaných elektronický dokument
SHA	Informační technologie	Secure hash algorithm
SID	Informační technologie	
SLA	Obecné	Service Level Agreement
SMB	Informační technologie	Server Message Block
SOAP	Informační technologie	Simple Object Access Protocol
SoD	Informační systémy	Segregation of Duty

Termín	Typ	Význam
SPO	Obecné	Společně posuzované osoby
SPRSS	Obecné	Střednědobé plánování rozvoje sociálních služeb
SpS	Informační systémy	Spisová služba
SQL	Informační technologie	Structured Query Language
SŘ	Obecné	Správní řízení dle ZSŘ
SS	Obecné	Sociální služby poskytované PSS
SSL/TLS	Obecné	SSL/TLS protocol
SSO	Informační technologie	Single Sign On
SSP	Obecné	Státní sociální podpora
SUIP	OVM	Státní Úřad Inspekce Práce
SÚIP“	Obecné	Státní úřad inspekce práce
SÚPM	Obecné	Společensky účelná pracovní místa
SVČ	Obecné	Samostatná výdělečná činnost
SW	Informační systémy	Software
UDDI	Informační technologie	Universal Description, Discovery and Integration
UML	Informační technologie	Unified Modeling Language
UoZ	Obecné	Uchazeč o zaměstnání - uchazečem o zaměstnání je fyzická osoba, která požádá o zprostředkování vhodného zaměstnání krajskou pobočku ÚP, v jejímž územním obvodu má bydliště a při splnění zákonem stanovených podmínek je krajskou pobočkou ÚP zařazena do evidence uchazečů o zaměstnání.
ÚP	OVM	Úřad práce
ÚP ČR	OVM	Úřad práce České republiky
ÚPS	Informační technologie	***U****ninterruptible* ***P****ower* ***S****upply (****S****ource*) – „nepřerušitelný zdroj energie!
Ústav	Obecné	Ústav (zařízení) pro péči o děti nebo mládež ve smyslu ZoSSP
VPM	Obecné	Volné pracovní místo
VPN	Informační technologie	Virtuální privátní síť
VPP	Obecné	Veřejně prospěšné práce
VS	Obecné	Veřejná služba
VS	Informační technologie	Virtuální server
WAN	Informační technologie	Wide Area Network
WDM	Informační technologie	Vlnový multiplex
WF	Obecné	Workflow
WINS	Informační technologie	
WS	Informační technologie	Web Services - Webová Služba.
WSDL	Informační technologie	Web Services Description Language)
WSUS	Informační technologie	Windows Server Update Service
XML	Informační technologie	Extensible Markup Language
XSD	Informační technologie	XML Schema Definition
XSLT	Informační technologie	eXtensible Stylesheet Language Transformations
ZKŘ	Předpis	Předpis č. 255/2012 Sb. Zákon o kontrole (kontrolní řád)
ZDP	Obecné	Zaručená doba provozu
ZMK	Obecné	Zaměstnanecká karta
ZoDP	Předpis	Předpis č. 586/1992 Sb. Zákon České národní rady o daních z příjmů

Termín	Typ	Význam
ZoFK	Předpis	Předpis č. 320/2001 Sb. Zákon o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole)
ZoHN	Předpis	Předpis č. 111/2006 Sb. Zákon o pomoci v hmotné nouzi
ZoISVS	Předpis	Předpis č. 365/2000 Sb. Zákon o informačních systémech veřejné správy a o změně některých dalších zákonů
ZoISVSnov	Předpis	Předpis č. 81/2006 Sb. Zákon, kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, a další související zákon
ZoOZPNZ	Předpis	Předpis č. 118/2000 Sb. Zákon o ochraně zaměstnanců při platební neschopnosti zaměstnavatele a o změně některých zákonů
ZoPDOZP	Předpis	Předpis č. 329/2011 Sb. Zákon o poskytování dávek osobám se zdravotním postižením a o změně souvisejících zákonů
ZoPř	Předpis	Předpis č. 200/1990 Sb. Zákon České národní rady o přestupcích
ZoSP	Předpis	Předpis č. 634/2004 Sb. Zákon o správních poplatcích
ZoSPOD	Obecné	Předpis č. 359/1999 Sb. Zákon o sociálně-právní ochraně dětí
ZoSS	Předpis	Předpis č. 108/2006 Sb. Zákon o sociálních službách
ZoSSP	Předpis	Předpis č. 117/1995 Sb. Zákon o státní sociální podpoře
ZoZ	Obecné	Zájemce o zaměstnání - Zájemcem o zaměstnání je fyzická osoba, která požádá o zprostředkování vhodného zaměstnání krajskou pobočku ÚP, kdekoliv na území ČR a při splnění zákonem stanovených podmínek je krajskou pobočkou ÚP zařazena do evidence zájemců o zaměstnání.
ZoZam	Předpis	Předpis č. 435/2004 Sb. Zákon o zaměstnanosti
ZoŽEM	Předpis	Předpis č. 110/2006 Sb. Zákon o životním a existenčním minimu
ZP	Předpis	Předpis č. 262/2006 Sb. Zákon zákoník práce
ZPD	Obecné	Zaručená provozní doba
ZR	Obecné	Základní registry
ZS	Obecné	Zaměstnavatelský subjekt
ZSŘ	Předpis	Předpis č. 500/2004 Sb. Zákon správní řád
ZZ	Obecné	Zahraniční zaměstnanost
ZZR	Předpis	Předpis č. 111/2009 Sb. Zákon o základních registrech