



Čj. 28253/2020-UVCR-3

VÝZVA K ÚČASTI NA PŘEDBĚŽNÉ TRŽNÍ KONZULTACI

včetně zadávací dokumentace k nadlimitní veřejné zakázce s názvem:

„Zajištění softwarové části akreditačního systému pro předsednictví ČR v Radě EU v roce 2022“

Česká republika – Úřad vlády České republiky (dále jen „zadavatel“) Vás vyzývá k účasti na předběžné tržní konzultaci, konané dle § 33 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „ZZVZ“), za účelem získání informací relevantních pro stanovení předpokládané hodnoty veřejné zakázky dle 16 odst. 6 ZZVZ, přípravu zadávacích podmínek a informování potenciálních dodavatelů o záměru a požadavcích na zadání shora jmenované veřejné zakázky.

A. Požadavky na zadávací podmínky

1. Identifikační a kontaktní údaje zadavatele

Název: Česká republika – Úřad vlády České republiky
Sídlo: nábr. E. Beneše 128/4, 118 01 Praha 1 – Malá Strana
IČO: 00006599
DIČ: CZ00006599
Zastoupená: PhDr. Štěpán Černý, ředitel Odboru koordinace evropských politik
Sekce pro evropské záležitosti
Kontaktní osoba: Mgr. Lenka Dudová, Oddělení veřejných zakázek

2. Vymezení druhu, režimu a předmětu veřejné zakázky

2.1 Předmět veřejné zakázky

Předmětem veřejné zakázky je zajištění akreditačního systému pro předsednictví ČR v Radě EU v druhé polovině roku 2022 (dále jen „CZ PRES 2022“) ze strany Úřadu vlády jakožto centrálního koordinátora pro zajištění příprav a výkonu předsednictví, ve smyslu usnesení vlády č. 729 ze 14. října 2019, k zajištění příprav předsednictví České republiky v Radě Evropské unie pro rok 2020 a střednědobého výhledu finančního a personálního zajištění výkonu předsednictví České republiky v Radě Evropské unie pro roky 2021 – 2023.

Účelem veřejné zakázky je zajistit akreditační systém, prostřednictvím kterého se budou akreditovat účastníci jednotlivých jednání pro akce konané na území ČR během CZ PRES 2022. Nad rámec toho by akreditační systém měl umožnit zadávat služby související s organizačním a logistickým zajištěním zasedání (tj. např. logistika přepravy delegátů pomocí oficiálních konvojů, zajištění cateringu, ubytování delegátů, přehled doprovodného programu zasedání, přehled požadavků na technické vybavení konferenčních prostor). U vybraných akcí budou data ze systému také využívána bezpečnostními složkami ČR za účelem prověřování osob.

Počet akcí, ke kterým bude akreditační systém využíván, bude v rozsahu přibližně 250. Akreditační systém bude určeným informačním systémem veřejné správy, neboť se předpokládá přístup cca 25 000 akreditovaných osob.

Veřejná zakázka na akreditační systém bude rozdělena na dvě části zadávané v samostatných zadávacích řízeních. Softwarová část bude řešena pořízením existujícího

softwarového řešení, které bude přizpůsobeno potřebám předsednictví, nebo naprogramováním nového řešení, a to v závislosti na výsledku předběžných tržních konzultací. Hardwarové řešení bude zajištěno samostatně, a to s využitím již existující infrastruktury státní správy.

Bližší požadavky na akreditační systém jsou uvedeny v příloze č. 1 této výzvy.

Bližší informace o parametrech a funkcionalitě hardwaru, na kterém bude akreditační systém provozován, jsou uvedeny v příloze č. 2 této výzvy.

2.2 Druh a režim veřejné zakázky

Nadlimitní veřejná zakázka na služby.

2.3 Klasifikace veřejné zakázky

72000000-5	Informační technologie: poradenství, vývoj programového vybavení, internet a podpora
72200000-7	Programování programového vybavení a poradenské služby
72260000-5	Služby programového vybavení
72261000-2	Podpora programového vybavení
72320000-4	Databázové služby
72321000-1	Databázové služby s přidanou hodnotou

2.4 Místo plnění veřejné zakázky

Místo plnění veřejné zakázky je Praha.

2.5 Doba plnění veřejné zakázky

Doba plnění veřejné zakázky: Předpokládaná doba zahájení plnění veřejné zakázky je v závislosti na průběhu zadávací řízení od července 2021. Akreditační systém musí být v plném provozu od března 2022 do ledna roku 2023.

2.6 Předpokládaná hodnota veřejné zakázky

Účelem předběžné konzultace je rovněž stanovení předpokládané hodnoty veřejné zakázky, resp. jejích dílčích částí. Zadavatel však předpokládá výdaje na zajištění akreditačního systému ve výši 4.000.000 Kč bez DPH.

B. Předběžné tržní konzultace

1. Vymezení předmětu a účelu předběžné tržní konzultace

Zadavatel s ohledem na charakter předmětu veřejné zakázky rozhodl využít možnosti vést předběžné tržní konzultace dle § 33 ZZVZ.

Předmětem předběžné tržní konzultace je především:

- stanovení předpokládané hodnoty veřejné zakázky;
- stanovení nejvýhodnější varianty plnění veřejné zakázky – pořízení existujícího softwarového řešení, úprava existujícího řešení pro potřeby předsednictví, vytvoření nového řešení pouze pro účely předsednictví;
- zjištění možností trhu – okruhu možných dodavatelů.

Zadavatel tímto způsobem hodlá předcházet možným rizikům, která by se při zadávání veřejné zakázky a jejím následném plnění mohla vyskytnout.

Zadavatel vypsáním předběžné tržní konzultace současně ověřuje ze strany dodavatelů možnosti nastavení zadávacích podmínek, a to zejména z hlediska vhodnosti a možné odezvy dodavatelů na zamýšlené zadávací podmínky.

Dodavatelé se budou moci k navrhovaným možnostem vyjádřit, čímž dojde ke zvýšení transparentnosti zadávacího řízení a získání relevantních a objektivních informací o možnostech trhu tak, aby zadavatel mohl optimálně nastavit zadávací podmínky veřejné zakázky, resp. celého zadávacího řízení, a umožnil tak optimální soutěž dodavatelů o veřejnou zakázku.

2. Podmínky účasti na předběžné tržní konzultaci a vymezení okruhu účastníků

Předběžná tržní konzultace je otevřena širšímu okruhu relevantních dodavatelů.

Předběžných tržních konzultací se mohou účastnit všichni dodavatelé nebo odborníci, kteří zvažují podání nabídky na veřejnou zakázku, a zadavatel nestanoví žádné další podmínky pro účast dodavatelů na jednání.

Účast na předběžné tržní konzultaci není zpoplatněna.

Předběžná tržní konzultace bude probíhat formou společného jednání zástupců dodavatelů na straně jedné a zástupců zadavatele na straně druhé.

Předběžná tržní konzultace bude vedena tak, aby to nenarušilo hospodářskou soutěž ani zásady zadávání veřejných zakázek uvedené v § 6 ZZVZ.

3. Průběh předběžné tržní konzultace

Z jednání bude pořizován audiozáznam.

Před jednáním budou vyžadovány identifikační údaje všech účastníků.

Z jednání bude vyhotoven zápis.

4. Lhůta, způsob a podmínky přihlášení do předběžné tržní konzultace

Dodavatelé, kteří mají o účast na předběžných tržních konzultacích zájem, nechť kontaktují Mgr. Lenku Dudovu na e-mailu verejnezakazky@vlada.cz nejpozději **do 04.11.2020 do 12:00 hod.**

Předběžné tržní konzultace se **nemohou účastnit neregistrovaní dodavatelé**. Registrace dodavatelů slouží pro potřeby rezervace místnosti o dostatečné kapacitě a za účelem zajištění dodržení pravidel přijatých vládou nebo zadavatelem za účelem omezení šíření onemocnění Covid 19.

5. Místo a termín konání předběžné tržní konzultace

Předběžná tržní konzultace formou osobního jednání bude zahájena **dne 05.11.2020 v 10:00 hod.** Předpokládaná délka trvání předběžné tržní konzultace jsou 2 hodiny.

Místo konání předběžné tržní konzultace bude na adrese **Lichtenštejnský palác, U Sovových mlýnů 506/4; Praha 1. Sraz účastníků před budovou v 9:50 hod.**

V případě, že v době konání předběžné tržní konzultace budou v České republice platit vládní opatření týkající se shromažďování osob k zamezení šíření onemocnění Covid 19 nebo budou taková omezení platná u zadavatele, uskuteční se předběžná tržní konzultace formou videokonference. Videokonference se mohou účastnit pouze registrovaní dodavatelé, kterým bude zaslán link pro přihlášení do videokonferenční místnosti. Registraci do videokonference je nutné provést do 05.11.2020 do 10:00 hod. Předběžná tržní konzultace formou videokonference se uskuteční dne 05.11.2020 do 13:00 hod. Registrovaní dodavatelé, si budou mít možnost ověřit připojení a nastavení techniky pro účast ve videokonferenci 05.11.2020 do 12:00 hod prostřednictvím obdrženého linku.

6. Práva zadavatele, ostatní podmínky

Zadavatel si vyhrazuje právo:

- komunikovat s dodavateli v českém jazyce;
- zaznamenávat průběh předběžné tržní konzultace prostřednictvím písemných a zvukových záznamů;
- dle § 36 odst. 4 ZZVZ identifikovat v zadávací dokumentaci osoby, které se podílely na předběžné tržní konzultaci; spolu s tímto zadavatel uvede všechny podstatné informace, které byly obsahem předběžné tržní konzultace;
- požadovat po dodavatelích doplnění či vysvětlení jimi předložených/poskytnutých informací;
- konat více než jedno ústní jednání k předběžné tržní konzultaci a provádět další jiné úkony zahrnující komunikaci s dodavateli;
- nehradit náklady dodavatele spojené s jeho účastí na předběžné tržní konzultaci;
- vyhodnotit a využít závěry předběžné tržní konzultace dle svého uvážení;
- ukončit předběžné tržní konzultace bez zpracování výsledků, a to i bez udání důvodů.

Případné dotazy a připomínky zasílejte pouze elektronicky na e-mail: verejnezakazky@vlada.cz.

Příloha č. 1: Požadavky na akreditační systém pro CZ PRES 2022

Příloha č. 2: Služby infrastruktury

V Praze

**PhDr.
Štěpán
Černý**

Digitálně podepsal
PhDr. Štěpán Černý
Datum: 2020.10.20
11:18:32 +02'00'

PhDr. Štěpán Černý,
ředitel Odboru koordinace evropských politik Sekce pro evropské záležitosti

Požadavky na akreditační systém pro CZ PRES 2022

Systém bude sloužit jako akreditační systém při pořádání akcí v rámci předsednictví České republiky v Radě EU v druhé polovině roku 2022, zejména pro provádění akreditací účastníků. Zvažováno je současné využití systému pro komplexní event management rozhraní a registraci služeb pro potřeby organizačního týmu. Systém bude použit jednorázově, výhradně pro účely předsednictví. Jednou z možných alternativ, vedle vybudování vlastního systému, je proto zakoupení dočasné licence na některý ze systémů dostupných na trhu a jeho přizpůsobení potřebám předsednictví.

Odhadovaný počet účastníků všech akcí: do 25.000;

Počet akcí: cca 250;

Funkčnost systému: od 3/2022 do konce roku 2022;

Počet osob používajících systém jako organizátoři: do 30 v rámci centrálního koordinátora (administrátor, pracovníci organizačního týmu, pracovníci v terénu), umožnění přístupu do akreditačního systému resortním koordinátorům – bude upřesněno, může jít o jednotky až desítky osob.

Způsoby použití:

Funkce související s akreditací účastníků

1) Akreditace účastníků

a. Typy akreditace:

- i. Pracovník centrálního koordinátora zadá základní údaje o osobě do systému a odešle pozvánku. Systém vygeneruje email s linkem na stránku pro akreditaci účastníka s daným emailem. Jde o neveřejnou webovou stránku (ENG/CZE), kde účastník nebo asistent vyplní požadované údaje a odešle žádost o akreditaci
 - ii. Novinář/účastník z řad veřejnosti - veřejná webová stránka (ENG/CZE), kde novinář/účastník z řad veřejnosti vyplní požadované údaje a odešle žádost o akreditaci
 - iii. Obslužný personál a řidiči – zadání do systému pracovníkem centrálního koordinátora;
- b. V případě některých typů akcí a účastníků paralelně odchází informace na Policii ČR, která provádí prověření – způsob předání informace o účastnících a vrácení informace o výsledku prověření bude specifikován;
- c. Po vrácení informace o výsledku prověření do systému systém změní stav akreditace účastníka a odešle účastníkovi email s potvrzením, že akreditace proběhla úspěšně/neúspěšně. Možnost editace stavu akreditace pro administrátory na straně centrálního koordinátora.

2) Přihlášení účastníka k akci

– *varianta, kdy se účastník může hlásit na více akcí;*

alternativa: na každou akci se účastník akredituje zvlášť skrze specifický odkaz – viz bod 1)

- a. Po odeslání žádosti o akreditaci bude účastníkům zobrazena stránka, kde budou moci provést výběr akcí, kterých se chtějí zúčastnit;

- b. Účastník si vybere jednu nebo více akcí;
- c. Účastníkovi je zaslán email s potvrzením akreditace pro akci a související informace.

3) **Akreditace a přihlášení na akci pro skupinu účastníků** – řešení pro situaci, kdy jednu osobu nebo skupinu osob (delegaci) přihlašuje na akci jiná osoba – v takovém případě je možné skupinové zadání a skupinové přihlášení všech účastníků na akce. Součástí skupinového zadání je určení správce delegace a určení, zda potvrzovací údaje o akreditaci a přihlášení k akci chodí pouze jemu nebo také na všechny členy delegace (u osob, které nejsou v roli správce, v tomto případě mail obsahuje odkaz na stránky pro přihlášení k akci pro danou osobu – např. pro možnost individuálního programu).

4) **Tvorba badge pro prokázání akreditace**

- a. Badge je nepřenositelný, obsahuje základní info. o osobě, foto, prostředek pro kontrolu platnosti (např. QR kód, RFID);
- b. Distribuci badge zajišťuje organizátor – pro jednu osobu může existovat pouze jeden platný badge;
- c. Organizátor má možnost zneplatnit badge a vytvořit nový (náhradní).

5) **Kontrola badge při vstupu na akci**

- a. Organizátor „v terénu“ je vybaven zařízením pro načtení badge dle navržené technologie – je třeba zohlednit dostupné technické vybavení státní správy;
- b. Na zařízení je zobrazeno, zda má účastník oprávnění pro vstup na akci.

Funkce související s administrací akcí na straně organizátora – event management rozhraní

6) **Organizace akcí**

- a. Organizátoři mají k dispozici komplexní pohled na účastníky, akce a lokality – vidí všechny jejich vazby a mohou generovat jejich seznamy;
- b. Organizátoři mají k dispozici kalendář pro zobrazení akcí a lokalit a jejich správu (vytvoření akce, přesunutí akce do jiné lokality, zrušení akce), vidí informace o požadavcích na catering (vč. např. zvláštních dietních požadavků), technické vybavení místností apod.;
- c. Účastníkům akce je možno hromadně odeslat email s informacemi o akcích a jejich změnách;
- d. Organizátor má možnost zadávat, měnit, mazat údaje o účastnících, akcích, lokalitách, vozidlech, etc.

7) **Organizace přepravy**

- a. Organizátoři přiřazují k akcím vozidla (ze seznamu všech volných vozidel – dle kalendáře jejich využití) a následně k nim přiřazují řidiče (opět dle seznamu, resp. kalendáře dostupných řidičů);
- b. Vhodné nastavení automatické kontroly a chybové notifikace tak, aby akce byla pokryta vozidly, dle počtu účastníků a počtu míst ve vozidlech, a aby vozidla byla obsazena řidiči.

8) **Zajištění ubytování** – bude specifikováno po vysoutěžení dodavatelů ubytovacích služeb, zvažované varianty:

- a. Minimální – v emailu s přihlášením k akci bude seznam odkazů na stránky hotelů, kde si účastník sám provede rezervaci ubytování;
- b. Maximální – na webové stránce účastníka bude zobrazení dostupných volných kapacit a bude zde přímo možné provést rezervaci, tj. předpoklad propojení s rezervačními systémy poskytovatelů ubytování.

Zvláštní požadavky:

Je třeba zajistit vysokou úroveň zabezpečení z hlediska kybernetické bezpečnosti, postupovat v souladu s požadavky a doporučeními Policie ČR, NÚKIB, aj., systém musí být v souladu s pravidly dle GDPR.

Systém by měl umožnit logování provedených změn.

Webové rozhraní systému musí fungovat ve všech obvyklých webových prohlížečích.

SLUŽBY INFRASTRUKTURY

Obsah

Obsah	9
Seznam tabulek	10
1 Úvod	11
1.1 Cíl dokumentu	11
1.2 Pojmy a zkratky	11
2 Prostředí provozu aplikací	14
2.1 Základní vlastnosti ICT prostředí	14
2.2 Specifikace provozované infrastruktury	15
2.2.1 Výpočetní výkon	15
2.2.2 Diskový prostor	20
2.2.3 Zálohování	22
3 Poskytované služby infrastruktury	23
3.1 Hardware	23
3.2 Software	23
3.2.1 Pravidla pro využití SW komponent	23
3.2.2 Operační systémy	26
3.2.3 Databáze	28
3.3 Definice služeb infrastruktury	30
3.3.1 Infrastrukturní služby na úrovni OS	30
3.3.2 Diskové infrastrukturní služby	38
4 Průřezové služby infrastruktury	39
4.1 DNS	39
4.2 NFS	39
4.3 DHCP	39
4.4 Mailové služby	39
4.5 VPN	39
4.6 LoadBalancing	40
4.7 Firewall	40
4.8 Proxy	40
4.9 ServiceDesk	40
4.10 Provozní dohled	41
4.11 Bezpečnostní monitoring	41
4.12 Testy	41
5 Architektonické principy	42
5.1 Pravidla pro návrh architektury řešení	42
5.1.1 Adaptabilita a flexibilita	42
5.1.2 Standardizace procesů rozvoje a podpory	42
5.1.3 Bezpečnost	43
5.1.4 Náklady na vlastnictví a provoz	43
5.1.5 Dokumentace	43
5.2 Základní rysy architektury	44
5.2.1 Škálovatelnost	44
5.2.2 Dostupnost	44
5.2.3 Monitorování a varování	44
5.2.4 Zálohování a obnova	44
5.3 Preferované architektonické patterny	44
5.3.1 Samostatný virtuální server	44
5.3.2 Vysoká dostupnost mezi datovými centry	46

Seznam tabulek

Tabulka 1 – Technické parametry infrastrukturních služeb x64.....	17
Tabulka 2 – Technické parametry infrastrukturních služeb Power	19
Tabulka 3 – Technické parametry infrastrukturních služeb Diskových prostorů	21
Tabulka 4 – Technické parametry infrastrukturních služeb zálohování	23
Tabulka 5 – Infrastrukturní služby OS MS Windows 2018 Server	30
Tabulka 6 – Infrastrukturní služby OS RedHat Enterprise Linux na platformě x86	31
Tabulka 7 – Infrastrukturní služby OS RedHat Enterprise Linux na platformě Power	32
Tabulka 8 – Infrastrukturní služby OS IBM AIX.....	34
Tabulka 9 – Infrastrukturní služby MS SQL 2016 Server	35

1 Úvod

1.1 Cíl dokumentu

Cílem dokumentu je poskytnout ucelený přehled služeb poskytovaných v ICT prostředí státního podniku [REDACTED] dále Poskytovatel infrastruktury) pro účely hostování informačních systémů provozovaných zde Úřadem Vlády (dále Objednatel). Dokument si klade za cíl popsat množinu poskytovaných infrastrukturních služeb a vytvořit vzory pro jejich výběr tak, aby z nich bylo možné vybírat požadované služby ICT prostředí v rámci výběrových řízení Objednatele. Každá definice služby popisuje její vlastnosti, rozsah, možnou návaznost na další služby a současně také bodové ohodnocení (na způsob interní úměry ceně poskytované služby) pro hodnocení plnění nabídky ve výběrovém řízení. Účastník výběrového řízení (dále Dodavatel) připraví na základě těchto služeb návrh architekturu infrastruktury způsobem popsáním níže.

1.2 Pojmy a zkratky

Termín	Význam
AD	Microsoft Active Directory
AIX	Unixový operační systém vyráběný společností IBM
BB	building block
BM	bezpečnostní monitoring
CMS2	Privátní síť spravovaná [REDACTED]
CPU	Central Procesor Unit
DB	Databáze, informační systém nebo služby určená pro ukládání a správu dat
DC	Datové centrum
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DR	Disaster Recovery
EPS	Events Per Second – jednotka účtování služby bezpečnostní monitoring (počet odeslaných logů do SIEM za vteřinu)
F5	Aplikační firewall
FC	Fibre Chanel
FPM	Flows Per Minute – pomocná jednotka služby bezpečnostní monitoring (počet uskutečněných spojení za minutu)
GOVBONE	Privátní síť spravovaná [REDACTED]
HW	Hardware
IBM VMRM DR	IBM Virtual MACHine Recovery Manager, Disaster Recovery. Nástroj pro implementaci DR na platformě IBM Power
IRP	Incident response platform – platforma pro zpracovávání a evidenci kybernetických incidentů

Termín	Význam
JBS	Jednotný bezpečnostní systém
KVM	Hardwarové zařízení, které umožňuje uživateli ovládat více počítačů z jedné klávesnice, monitoru a myši
LAN	Local Area Network
Logický diskový objem	Virtuální diskový prostor alokovaný z diskového pole nebo celkového sdíleného diskového prostoru formátovaný do podoby logického disku nebo skupiny logických disků
NFS	Network File Systém
OS	operační systém
Power	Serverová platforma založená na procesorech Power společnosti IBM
PowerVM	Virtualizační platforma, provozovaná na prostředí Power
QNI	QRadar Network Insights – doplňkový modul SIEMu pro monitoring síťového provozu na vyšších vrstvách
RAM	Random Access Memory
RHEL	Unixový operační systém distribuovaný společností RedHat
SAN	Storage Area Network
SD	Aplikace Service Desk
SD	Service Desk
SLA	Service Level Agreement – dohodnutá pravidla podpory/služby
SLA Critical	Dostupnost 99,99 %, Provozní doba pod SLA: 24x7, maximální kumulovaný výpadek 52 min/rok, jednotlivý výpadek max 15 min
SLA High	Dostupnost 99,9 %, Provozní doba pod SLA: 24x7, maximální kumulovaný výpadek 43 min/měsíc
SLA Medium	Dostupnost 99,45 %, Provozní doba pod SLA: 24x7, maximální kumulovaný výpadek 4 hod/měsíc
SP	IBM Spectrum Protect
SPP	IBM Spectrum Protect Plus
STOR1	Typ infrastrukturní služby diskového úložiště
STOR3	Typ infrastrukturní služby diskového úložiště
SW	Software
TCO	Total Cost of Ownership
TSM	Tivoli Storage Manager
UPS	nouzový zdroj napájení infrastruktury
VLAN	Virtuální LAN, logicky nezávislá síť v rámci jednoho nebo několika zařízení
VMware	Virtualizační platforma, provozovaná na prostředí x64
VPN	Virtual Private Network
WAN	Wide Area Network
WH	Workhours

Termín	Význam
WIN	Windows
x64	Serverová platforma založení na 64bitových procesorech Intel

2 Prostředí provozu aplikací

Objednatel bude provozovat poptávaný informační systém na infrastruktuře pořízené formou služeb infrastruktury, které objednává poskytovatele těchto služeb, kterým je Poskytovatel infrastruktury.

Tato kapitola popisuje pravidla, parametry a ostatní podmínky služby. Dodržení podmínek služby poskytování infrastruktury, definovaná Poskytovatelem infrastruktury, je podmínkou dodání informačního systému (IS) a jeho provozu v rámci tohoto prostředí.

2.1 Základní vlastnosti ICT prostředí

ICT prostředí Poskytovatele infrastruktury je provozováno ve dvou oddělených datových centrech (DC).

Služby poskytování infrastruktury v jednotlivých DC jsou implementovány a provozovány tak, aby byl v každém okamžiku (při plánovaných i neplánovaných výpadcích) zachován provoz Služeb alespoň v jednom fyzickém DC. Tento princip umožňuje Dodavateli budovat architekturu IS s různou úrovní dostupnosti s využitím technologií umístěných v různých DC. To ve zkratce naplňuje následující základní architektonické principy:

- samostatná n-úrovňová aplikace provozovaná ve virtualizovaném prostředí platformy x64 v jednom DC;
- samostatná n-úrovňová aplikace provozovaná ve virtualizovaném prostředí platformy IBM Power v jednom DC;
- zvýšená úroveň dostupnosti aplikace provozované ve virtualizovaném prostředí (řešeno cluster-like technologiemi dané platformy);
- zvýšená úroveň dostupnosti aplikace provozované ve virtualizovaném prostředí (řešeno cluster-like technologiemi) se zajištěním klonování logických diskových objemů v rámci jednoho DC;
- zvýšená úroveň dostupnosti aplikace provozované ve virtualizovaném prostředí (řešeno cluster-like technologiemi dané platformy) se zajištěním replikace logických diskových objemů mezi diskovými poli v různých DC;
- vysoká dostupnost aplikace provozované ve virtualizovaném prostředí v režimu active-passive v obou DC s online prováděnou datovou replikací a s možností transparentního přesunu dat a aplikace mezi oběma DC v případě vzniku poruchy nebo havarijní situace;
- pro všechny výše popisované alternativy jsou k dispozici základní zálohovací služby viz popis níže.

Parametry jednotlivých DC:

- základní technologie (UPS, WAN, LAN, přídavné chlazení, KVM, trezory pro zálohy, datové rozvaděče – rack);

- vzduchotechnika a chlazení;
- energie pro provoz zařízení a chlazení;
- náhradní zdroje napájení;
- řídicí systémy pro technologie;
- stabilní hasicí zařízení;
- výkon dohledu non-IT technologií v režimu 7 × 24 hod.

Fyzická bezpečnost DC:

- elektronický přístupový systém s kontrolou vstupu do jednotlivých bezpečnostních oblastí;
- uzavřený kamerový systém ve všech technologických prostorech a na plášti budov s ukládáním vybraných záznamů;
- elektronická zabezpečovací signalizace;
- výkon činnosti ozbrojené ostrahy v režimu turnusových nepřetržitých dvanáctihodinových směn (7 × 24 hod);
- součástí zajišťování objektové bezpečnosti a řízeného přístupu je i zajištění provozu a servisu Jednotného bezpečnostního systému (JBS), vytvoření a aktualizace bezpečnostní dokumentace a zajištění bezpečnosti ICT;
- odolnost objektu vůči náloži až 10 kg TNT.

2.2 Specifikace provozované infrastruktury

Níže je uveden stručný a orientační přehled technických parametrů dostupných služeb infrastruktury.

2.2.1 Výpočetní výkon

Servery jsou poskytovány v několika různých variantách, formou dedikovaného výpočetního výkonu. Varianty poskytování výpočetního výkonu je nutné rozlišovat

- z pohledu způsobu přidělení výpočetního výkonu (a datového prostoru),
- s ohledem na zvolenou/dostupnou výpočetní platformu (architekturu CPU).

Aktuálně jsou k dispozici varianty alokace výpočetního výkonu založené na platformě x64 a na RISC platformě Power. Výpočetní výkon je nabízen na úrovni níže popsanych služeb ve virtualizovaném prostředí:

- virtualizované servery x64;
- virtualizované servery IBM Power.

Služby infrastruktury založené na fyzických strojích nejsou provozovány, je možné využívat pouze variant služeb infrastruktury založených na virtualizaci.

Alokace výpočetního výkonu, resp. jeho zohlednění pro potřeby návrhu architektury v rámci předkládané nabídky, probíhá formou definice požadovaných služeb v Příloze 7 - Infrastrukturní požadavky Dodavatele.

2.2.1.1 Výpočetní výkon na platformě x64

Standardem je 64bitová platforma x86. V každém datovém centru je umístěno jedno nebo více Blade center. Jednotlivé Blade systémy mají 2 CPU sockety. V každém DC je alokováno 20 % záložních zdrojů (Blades) pro zajištění vysoké dostupnosti.

Platforma výpočetního výkonu nemá interní disky, je připojena ke službám poskytování diskových prostorů (definice služeb poskytování diskového prostoru STOR1 a STOR3). Konektivita k diskovému úložišti je zajištěna pomocí redundantního FibreChannel (FC) propojení.

Služby zahrnují služby DC včetně prostoru a energií.

Virtualizační platforma je provozována na technologii VMware v minimální verzi VMware vSphere 6.7. Součástí služby jsou SW licence virtualizační platformy a aktualizace verzí virtualizačního SW. Na úrovni virtualizace jsou fyzická jádra mapována na virtuální CPU (vCPU) (v nejhorším případě) v poměru 1:10 (upozorňujeme, že definice služeb je založena na přidělení vCPU).

Alokace je realizována prostředky VMware a je v odpovědnosti Poskytovatele infrastruktury.

Mapování RAM je prováděno použitím v tzv. Building bloků (BB) a není agregované (1 GB vRAM = 1 GB RAM). Pro označení BB je používán poměr přidělení RAM (GB) na ekvivalent jednoho vCPU:

- BB 1:4 jsou určeny pro provoz virtuálních serverů s OS Windows, a
- BB 1:2 jsou určeny pro provoz virtuálních serverů s OS Linux.

Jednotka obsahuje licence virtualizačního SW a instalace operačního systému v souladu s příslušnou službou infrastruktury.

Dodavatel navrhne do nabídky požadované virtuální servery, které konfiguruje pomocí infrastrukturních služeb definovaných Poskytovatelem infrastruktury..

V případě potřeby virtuálního serveru s jiným poměrem CPU a RAM, než je definovaný v rámci povolených služeb, použije Dodavatel variantu služby, která odpovídá parametru s vyšší hodnotou požadovaného parametru (např. při požadavku na virtuální server s OS Windows, 2 vCPU a 32 GB vRAM použije Dodavatel infrastrukturní službu s parametry 8 vCPU a 32 GB RAM).

Služby poskytování výpočetního výkonu zahrnují zejména následující služby:

- prvotní zajištění a instalaci virtualizovaného výpočetního systému;
- správu a údržbu HW a virtualizačního SW;
- návrh a správu platformy v rámci dohodnutých politik;
- proaktivní monitoring HW a virtualizačního SW a řešení incidentů;
- preventivní systémovou údržbu;
- správu připojení do LAN/SAN;
- instalaci a správu příslušného SW dle typu použité služby.

Replikované jednotky

Replikované varianty jednotek zajišťují vysokou dostupnost prostředky virtualizační platformy. Ke každému virtuálnímu serveru je alokován výpočetní výkon v Záložním DC. V případě výpadku zdrojů v Primárním DC dojde k obnovení provozu virtuálního serveru v Záložním DC (tuto službu zajišťuje VMware). Replikace se provádí na úrovni prostředků virtualizace a diskového pole a předpokladem je zdvojená alokace výpočetního výkonu a diskových prostorů STOR1 daného virtuálního serveru, která je součástí příslušné infrastrukturní služby. Replikace diskových prostorů do druhého DC se provádí prostředky virtualizace a je asynchronní.

Virtuální servery je možno použít ve všech síťových bezpečnostních zónách včetně DMZ.

Tabulka 1 – Technické parametry infrastrukturních služeb x64

Název jednotky	BB x64 1:2
Stručný popis	Virtualizovaný výpočetní výkon x64 1 vCPU: 2 GB vRAM
Měrná jednotka	Stavební blok (BB) 1 vCPU + 2 GB vRAM
Výkonnostní parametry	Provozováno na platformě CPU E5-2697 v4 (Broadwell) 2.30 GHz nebo výkonnější. Použité paměti jsou typu DDR4.
Dostupnost (roční)	99,5 %
Provozní doba	24x7

Název jednotky	BB x64 1:4
Stručný popis	Virtualizovaný výpočetní výkon x64 1 vCPU: 4 GB vRAM
Měrná jednotka	Stavební blok (BB) 1 vCPU + 4 GB vRAM
Výkonnostní parametry	Provozováno na platformě CPU E5-2630 v4 (Broadwell) 2.2 GHz nebo výkonnější. Použité paměti jsou typu DDR4.
Dostupnost (roční)	99,5 %
Provozní doba	24x7

Název jednotky	BB x64 1:2 replikovaný
Stručný popis	Virtualizovaný výpočetní výkon x64 1 vCPU: 2 GB vRAM s pasivní zálohou v druhém DC replikovanou prostředky virtualizace
Měrná jednotka	Stavební blok (BB) 1 vCPU + 2 GB vRAM
Vazby na ostatní jednotky	Obsahuje dvojici jednotek BB 1:2 ve dvou datových centrech. Odpovídající konfigurace diskových prostorů STOR1 je pro tuto variantu využití rovněž zdvojená ve dvou datových centrech.
Dostupnost (roční)	99,9 %
Provozní doba	24x7

Název jednotky	BB x64 1:4 replikovaný
Stručný popis	Virtualizovaný výpočetní výkon x64 1 vCPU: 4 GB vRAM s pasivní

	zálohou v druhém DC replikovanou prostředky virtualizace
Měrná jednotka	Stavební blok (BB) 1 vCPU + 4 GB vRAM
Vazby na ostatní jednotky	Obsahuje dvojici jednotek BB 1:4 ve dvou datových centrech. Odpovídající konfigurace diskových prostorů STOR1 je pro tuto variantu využití rovněž zdvojená ve dvou datových centrech.
Dostupnost (roční)	99,9 %
Provozní doba	24x7

2.2.1.2 Výpočetní výkon na platformě Power

V současné době je standardem platforma Power8 pro výpočetně náročné operace a platforma Power9 pro paměťově náročné aplikace. Pro návrh infrastruktury a technické architektury budeme využívat platformu Power9.

V každém DC je umístěno několik serverů pSeries 850. Jednotlivé servery mají 4 CPU sockety (3 obsazené).

Platforma výpočetního výkonu nemá interní disky, je připojena ke službám poskytování diskových prostorů (definice služeb poskytování diskového prostoru STOR1). Konektivita k diskovému úložišti je zajištěna pomocí redundantního FibreChannel (FC) propojení.

Služby zahrnují služby DC včetně prostoru a energií.

Virtualizační platforma je provozována na technologii Power Virtual Machine (PowerVM) ve verzi PowerVM VIOS 2.6 či vyšší. Součástí služby jsou SW licence virtualizační platformy a aktualizace verzí virtualizačního SW.

Mapování RAM je prováděno použitím v tzv. Building bloků (BB). Pro označení Building bloků je používán poměr přidělení RAM (GB) k jednomu fyzickému CPU jádru Power9 (upozorňujeme, že definice služeb je založena na přidělení ekvivalentu fyzických CPU jader).

V současné době jsou podporovány:

- BB 1:50 jsou určeny pro provoz virtuálních serverů s OS AIX a OS Linux RHEL a jsou určeny pro provoz výkonově náročných aplikací,
- BB 1:80 jsou určeny pro provoz virtuálních serverů s OS Linux RHEL a jsou určeny pro provoz paměťově náročných aplikací.

Poskytovaný CPU výkon je virtuálnímu serveru poskytován formou CPU vláken, jejichž počet je konfigurovatelný (v závislosti na možnostech PowerVM).

Jednotka obsahuje licence virtualizačního SW a instalace operačního systému v souladu s příslušnou službou infrastruktury.

Dodavatel navrhne do nabídky požadované virtuální servery, které konfiguruje pomocí infrastrukturních služeb definovaných Poskytovatelem infrastruktury.

V případě potřeby virtuálního serveru s jiným poměrem CPU a RAM použije Dodavatel variantu služby, která odpovídá parametru s vyšší hodnotou požadovaného parametru (např. při požadavku na virtuální server s OS RHEL, 1,5 CPU a 75 GB RAM použije Dodavatel službu virtuálního serveru s dedikovaným výkonem 2 CPU a 100 GB RAM).

Dedikovaný výpočetní výkon virtuálního serveru lze rozdělit na virtuální jádra dle možností Power VM virtualizace.

Služby poskytování výpočetního výkonu zahrnují zejména následující činnosti:

- prvotní zajištění a instalaci virtualizovaného výpočetního systému;
- správu a údržbu HW a virtualizačního SW;
- návrh a správu platformy v rámci dohodnutých politik;
- proaktivní monitoring HW a virtualizačního SW a řešení incidentů;
- preventivní systémovou údržbu;
- správu připojení do LAN/SAN;
- instalaci a správu příslušného SW dle typu použité služby.

Replikované jednotky

Replikované varianty jednotek zajišťují vysokou dostupnost prostředky virtualizační platformy. Ke každému virtuálnímu serveru je alokován výpočetní výkon v Záložním DC. V případě výpadku zdrojů v Primárním DC dojde k obnovení provozu virtuálního serveru v Záložním DC (tuto službu zajišťuje komponenta IBM VMRM – Geographically Dispersed Resiliency for IBM Power Systems). Replikace se provádí na úrovni prostředků virtualizace a diskového pole (tj. předpokladem je zdvojená alokace výpočetního výkonu a diskových prostorů STOR1 daného virtuálního serveru, která je součástí příslušné infrastrukturní služby). Replikace diskových prostorů do druhého DC se provádí prostředky diskových polí a je synchronní.

Virtuální servery je možno použít ve všech síťových bezpečnostních zónách včetně DMZ.

Tabulka 2 – Technické parametry infrastrukturních služeb Power

Název jednotky	BB Power9 1:50
Stručný popis	Virtualizovaný výpočetní výkon Power9 1 CPU: 50 GB RAM
Měrná jednotka	Stavební blok (BB) 1 CPU + 50 GB RAM
Výkonnostní parametry	Provozováno na platformě CPU Power9 3GHz nebo výkonnější. Použité paměti jsou typu DDR3.
Dostupnost (roční)	99,9 %
Provozní doba	24x7

Název jednotky	BB Power9 1:80
Stručný popis	Virtualizovaný výpočetní výkon Power9 1 CPU: 16 GB RAM
Měrná jednotka	Stavební blok (BB) 1 CPU + 80 GB RAM
Výkonnostní parametry	Provozováno na platformě CPU Power9 3,4GHz nebo výkonnější. Použité paměti jsou typu DDR4.
Dostupnost (roční)	99,5 %
Provozní doba	24x7

Název jednotky	BB Power9 1:50 Replikovaný
Stručný popis	Virtualizovaný výpočetní výkon Power9 1CPU: 50 GB RAM s pasivní zálohou v druhém DC replikovanou prostředky virtualizace
Měrná jednotka	Stavební blok (BB) 1 CPU + 50 GB RAM
Výkonnostní parametry	Provozováno na platformě CPU Power9 3GHz nebo výkonnější. Použité paměti jsou typu DDR3.
Dostupnost (roční)	99,9 %
Provozní doba	24x7

Název jednotky	BB Power9 1:80 Replikovaný
Stručný popis	Virtualizovaný výpočetní výkon Power9 1 CPU: 80 GB RAM s pasivní zálohou v druhém DC replikovanou prostředky virtualizace
Měrná jednotka	Stavební blok (BB) 1 CPU + 80 GB RAM
Výkonnostní parametry	Provozováno na platformě CPU Power9 3,4GHz nebo výkonnější. Použité paměti jsou typu DDR4.
Dostupnost (roční)	99,5 %
Provozní doba	24x7

2.2.2 Diskový prostor

Požadovaný diskový prostor lze alokovat ve dvou technicky a výkonově rozdílných logických objemech:

- STOR1;
- STOR3.

Služba STOR1 je realizována na diskových polích s primárně točivými disky v kombinaci s flash disky (cca 10-20 % objemu). Nad oběma druhy datových úložišť pracuje auto-tiering, který se stará o to, aby nejvytíženější bloky dat byly umístěny na flash médiích a byl tak výrazně navýšen reálný výkon úložiště.

Služba STOR3 je realizována točivými disky (600 GB/10k SAS 2,5“) organizovanými do RAID-5. STOR3 není vhodný pro více zatížené transakční aplikace, zejména databáze.

Připojení prostřednictvím SAN sítě Poskytovatele infrastruktury (protokol FC p2p – switched fabric) umožňuje maximálně využít výkonové vlastnosti diskového pole. Tento způsob připojení je blokový. Toto připojení je určeno pro vysoké transakční zatížení. Veškeré použité komponenty jsou redundantní (řadiče, SAN switche, optické cesty).

Služby zahrnují služby datového centra včetně prostoru a energií.

Služby poskytování diskového prostoru zahrnují zejména následující činnosti:

- prvotní zajištění a instalaci HW a firmware diskových polí a SAN;
- konfigurace diskových jednotek a portů, konfigurace a správa RAID, tiering, zonu;
- správu a konfiguraci storage zařízení;

- posouzení vlivu na všechny provozované služby;
- proaktivní monitoring HW a řešení incidentů;
- preventivní systémovou údržbu;
- aktualizace firmware storage zařízení. (controllery, disky atd) na základě doporučení výrobce a s ohledem na stabilitu provozu;
- konfigurace a správa SAN protokolů a SAN prvků (optika Fibre Channel);
- vytváření a úpravu LUNs a Volumes a jejich mapování pro servery;
- diagnostiku a testování storage zařízení, řešení nestandardních a chybových stavů;
- generování reportů využití kapacit a analýza vytíženosti storage zařízení.

Replikované jednotky

Replikované varianty jednotek zajišťují vysokou dostupnost prostředky synchronní replikace diskových polí nebo asynchronní replikace prostředky virtualizační platformy (v závislosti na použité virtualizační platformě). Ke každému bloku STOR1 jednotek je alokován záložní blok STOR1 ve druhém DC a je nastavena replikace diskových prostorů. Replikace se provádí na úrovni jednotlivých volume (jeden filesystém nebo jeden diskový prostor připojený k serveru) nebo celých virtuálních serverů, všechny jednotky daného volume nebo všechny připojené volume daného virtuálního serveru musí být STOR1 redundantní.

Propustnost replikační linky mezi DC je minimálně 8 Gbit.

Nastavení replikace pro služby STOR3 není podporováno.

Tabulka 3 – Technické parametry infrastrukturních služeb Diskových prostorů

Název	STOR1
Stručný popis	Diskový prostor STOR1
Měrná jednotka	GB (1024 ³ bytes)
Výkonnostní parametry	Parametry provozní platformy jako celku: Pro soubory o velikosti 500 GB pole dosahuje min. 15000 IOPS pro zápis a 35000 IOPS pro čtení a propustnost 2000 MB/s. Doba odezvy průměrná: 0,6 ms Doba odezvy ve špičkách (dle současného zatížení): do 6 ms
Dostupnost (roční)	99,5 %
Provozní doba	24x7

Název	STOR3
Stručný popis	Diskový prostor STOR3
Měrná jednotka	GB (1024 ³ bytes)
Výkonnostní parametry	Parametry provozní platformy jako celku: Nejsou poskytovány garance propustnosti nebo IOPS. Průměrné hodnoty jsou až 10 000 IOPS na 250 GB pro zápis a propustnost 650 MB/s. Doba odezvy průměrná: 2-3 ms Doba odezvy ve špičkách (dle současného zatížení): do 12 ms
Dostupnost (roční)	99,5 %
Provozní doba	24x7

Název jednotky	STOR1 replikovaný
Stručný popis	Diskový prostor STOR1 replikovaný do druhého datového centra
Měrná jednotka	GB (1024 ³ bytes)
Vazby na ostatní jednotky	Obsahuje dvojici jednotek STOR1 ve dvou datových centrech.
Dostupnost (roční)	99,9 %
Provozní doba	24x7

2.2.3 Zálohování

Služba Operativní záloha popisuje standardizovanou jednotku zálohování.

Služba zálohování je poskytována pomocí software IBM Spectrum Protect (dříve Tivoli Storage Manager, TSM) s využitím principu deduplikace. SW licence zálohovacího systému jsou součástí služby. Součástí služby jsou i aktualizace verzí zálohovacího SW.

Konkrétně jsou používány tyto nástroje:

- IBM Spectrum Protect Plus (SPP) pro prostředí VMware;
- IBM Spectrum Protect (SP – dříve TSM) pro prostředí Power.

Jednotka je definována na základě objemu zdrojových dat zálohovaných 7x týdně jako logický full backup s retencí max. 28 dnů a změnovostí do 20 % týdně a zároveň do 10 % denně. Zdrojová data musí být nekomprimovaná a nešifrovaná v bodě a okamžiku převzetí zálohovacím systémem.

Službu lze použít na zálohování filesystémů a databází kompatibilních s použitou technologií zálohování.

Předpokladem efektivního poskytování služby je definice backup plánů ve spolupráci Objednatele, Dodavatele a Poskytovatele infrastruktury při uvážení požadavků na rovnoměrné vytížení a využití zálohovací platformy.

Služby zálohování zahrnují zejména následující činnosti:

- Správa páskových a diskových knihoven a deduplikačních apliančí;

- HW správa a konfigurace storage zařízení používaných pro zálohovací platformu;
- Obsluha zálohovacích technologií.

Tabulka 4 – Technické parametry infrastrukturních služeb zálohování

Název jednotky	Operativní záloha
Stručný popis	Běžná operativní záloha diskových prostorů s retencí 4 týdny
Měrná jednotka	Objem zálohovaných dat v GB (1024^3 bytes)
Výkonnostní parametry	Parametry provozní platformy jako celku: Propustnost zálohování (průměrná) 1200 MB/s. Propustnost obnovy (průměrná) 800 MB/s.
Provozní doba	24x7

3 Poskytované služby infrastruktury

Tato kapitola definuje služby, které může Dodavatel použít při návrhu infrastruktury a SW architektury nabízeného IS.

Pro jednotlivé služby jsou definovány podmínky a pravidla, která definují jejich technické, provozní a organizační parametry. Tyto parametry vychází z pravidel provozu DC Poskytovatele infrastruktury a není možné je měnit bez souhlasu [REDACTED]

3.1 Hardware

Služby infrastruktury, tedy výpočetní výkon, diskový prostor a zálohování, jsou poskytovány podle specifikací uvedených v kapitole 2.2. Specifikace provozované infrastruktury.

3.2 Software

Tato kapitola popisuje SW komponenty, které jsou součástí dodávaných služeb Poskytovatele infrastruktury. Popsané služby jsou součástí poskytovaných služeb a jejich využití je závislé na způsobu zajištění těchto služeb.

3.2.1 Pravidla pro využití SW komponent

3.2.1.1 Licence

Licence, nutné pro zajištění služby, jsou vždy její součástí.

Licence všech ostatních softwarových produktů, které nejsou součástí služby, musí být zajištěny jako součást dodávky IS.

Objednatel zároveň upozorňuje, že softwarové licence, které jsou součástí služeb, jsou ošetřené s ohledem na licenční podmínky příslušného výrobce. Pro softwarové licence, které Dodavatel nabídne jako součást dodávky IS, musí být Dodavatelem garantováno, že nebudou závislé na metrikách, jejichž splnění by omezovalo provozní a organizační procesy Poskytovatele infrastruktury (např. licence pro SW produkty, které jsou vázány na fyzické CPU).

3.2.1.2 Verze

U všech SW komponent, používaných jako součást služeb, je dodržováno pravidlo průběžné aktualizace. V rámci služeb jsou provozovány aktuální uvolněná nebo maximálně jedna předchozí uvolněná verze (pro hlavní verzi – major release), případně aktuální nebo maximálně dvě předchozí uvolněné verze (pro vedlejší verzi – minor release).

Update či upgrade SW komponent, které jsou součástí služby, je prováděn jako součást řízení životního cyklu aplikací v rámci procesů podpory Poskytovatele infrastruktury a jsou součástí ceny služby. Poskytovatel infrastruktury stanovuje plán upgrade a update jím zpracovaných SW komponent, který projednává se Objednatelem a Dodavatelem tak, aby plánované činnosti minimálně zasahovaly do využívání služeb a procesů podpory IS a služeb, nicméně stále platí výše uvedené pravidlo podporovaných verzí softwaru.

Dodavatel se zavazuje, že při dodržování těchto pravidel, ať už během implementace nebo během podpory produktivního provozu, zajistí Poskytovatel infrastruktury plnou součinnost ve všech částech řešení, za které je odpovědný.

3.2.1.3 Autentizace a přístupy

Pro serverové komponenty platí předpoklad, že uživatelé na úrovni OS, DB nebo dalších poskytovaných služeb pro potřeby instalace, administrace nebo podpory provozu jsou vytvářeni, udržováni a spravováni Poskytovatelem infrastruktury a pomocí jeho nástrojů. Autentizace probíhá lokálně na úrovni serveru.

Oprávnění pro softwarové komponenty, které jsou součástí služeb Poskytovatele infrastruktury, jsou přidělována v souladu s požadavky instalovaných, resp. provozovaných aplikací, nicméně nejvyšší úroveň oprávnění (root, admin) nejsou přidělována mimo pracovníky Poskytovatele infrastruktury. V případě, že v rámci správy životního cyklu aplikace (instalace, upgrade) jsou tato oprávnění nezbytná pro provedení zásahu, jsou zajištěna prostřednictvím součinnosti Poskytovatele infrastruktury při zachování principu kontroly 4 očí.

Centrální služby správy uživatelů IS na úrovni administrace aplikace (IDM, LDAP nebo AD), pokud je Dodavatel potřebuje jako součást navržené architektury, musí být součástí dodávky nabízeného IS. Požadavky na správu uživatelů aplikace včetně jejich autentizace je součástí funkčních a technických požadavků poptávaného IS.

3.2.1.4 Síťová konfigurace

Pro zajištění síťové konektivity platí následující pravidla:

- Dodavatel připravuje návrh síťové architektury:
 - návrh síťové konfigurace (komponenty, VLAN, jména serverů, domén atd.);
 - návrh povolené komunikace (interní, externí);

- návrh kontrol komunikace aplikace na úrovni aplikačního firewallu F5 pro externí komunikaci;
- Dodavatel zajistí, že uvedené návrhy síťové architektury budou v souladu s pravidly Poskytovatele infrastruktury (bezpečnostní politiky, jmenné konvence, zadávací dokumentace atd.);
- návrh síťové architektury podléhá posouzení a schválení Objednatele a Poskytovatele infrastruktury;
- přidělování adresních prostorů a nastavení sdílených síťových služeb (DNS, firewall, aplikační firewall atd.) je v kompetenci Poskytovatele infrastruktury.

Při návrhu je nutné zohlednit následující pravidla:

- každý server je připojen minimálně ke dvěma nezávislým síťovým prostředím:
 - primární VLAN, která slouží pro vlastní komunikaci aplikací;
 - sekundární VLAN, která slouží pro administraci, monitoring, zálohování atd.;
- návrh síťového prostředí musí zohlednit segmentaci jednotlivých vrstev architektury tak, aby bylo možné oddělit provoz mezi jednotlivými vrstvami (optimálně vrstva uživatelského rozhraní, aplikační vrstva a databázová vrstva);
- externí komunikace je standardně povolována z prostředí veřejného internetu, CMS2 a GOVBONE (komunikační síť spravovaná Objednatelem);
- veškerá externí komunikace prochází aplikačním firewallem F5, komunikace z prostředí interní sítě Objednatele nebo Poskytovatele infrastruktury prochází aplikačním firewallem F5, pokud to způsob komunikace aplikace nebo obsah přenášených dat vyžaduje.

3.2.1.5 Landscape

Pro implementaci je standardně využíváno 3 úrovněového Landscape:

- vývojové prostředí je určené pro vývoj a nastavení funkcionalit systému, prostředí je ve správě Dodavatele. Konfigurace prostředí je obvykle minimalistická a zaměřená primárně na procesy vývoje;
- testovací prostředí je určené pro testování aplikací, a to jak z funkčního hlediska (testování funkcionalit systému), tak z pohledu chování aplikace v prostředí infrastruktury (např. testování vysoké dostupnosti nebo testy chování aplikace po upgradu nebo patchování infrastruktury). Konfigurace je shodná s produkčním prostředím, výkon prostředí může být omezen s ohledem na probíhající testy;
- produkční prostředí.

V případě, že aplikace obsahuje B2B rozhraní dostupné z externího prostředí, je doporučeno implementovat další testovací prostředí (testování třetích stran), které je určeno pro externí subjekty pro pravidelné, resp. ad-hoc testování datových formátů a používaných komunikačních standardů.

3.2.2 Operační systémy

3.2.2.1 Windows

Verze

Operační systém Windows je aktuálně provozován ve verzi Windows Server 2019 a Windows Server 2016.

Virtualizace

Pro běh logických serverů se používá prostředí VMware. Pro Dodavatele je způsob virtualizace transparentní a nemá možnost volit mezi virtualizačními platformami.

Doména

Centrální doména není používána. V případě, že aplikace vyžaduje funkcionalitu doménového řadiče, musí být tento implementován jako součást řešení Dodavatele.

Vysoká dostupnost

Vysoká dostupnost je standardně zajišťována prostředky virtualizační platformy.

Systémové zdroje

Pro návrh logických serverů s OS Windows je možné použít všechny poskytované druhy BB v kategorii BB x64 1:4 viz popis HW.

Minimální předepsaný diskový prostor je 100 GB zálohovaného diskového prostoru per server, který je nutné zohlednit při definici požadovaných služeb.

Bezpečnost a hardening

Hardening a bezpečnostní nastavení je provedeno standardně jako součást instalace, resp. jako součást instalace patchů dle standardů Poskytovatele infrastruktury.

Patchování

Verze OS je udržována na aktuální verzi, případně na dvou předchozích uvolněných vedlejších verzích.

Instalaci patchů provádí Poskytovatel infrastruktury za součinnosti Dodavatele. Termín nasazení navrhuje Poskytovatel infrastruktury nebo Dodavatel.

3.2.2.2 AIX

Verze

Operační systém AIX je aktuálně provozován ve verzi 7.2 nebo 7.1.

Virtualizace

Pro běh logických serverů se používá systémového nástroje IBM Power VM. Pro Dodavatele je způsob virtualizace transparentní a nemá možnost volit mezi virtualizačními platformami.

Vysoká dostupnost

Vysoká dostupnost je standardně zajišťována prostředky virtualizační platformy prostředí AIX, která je poskytována kombinací nástrojů LPM (Live Partition Mobility), SRR (Simplified Remote Restart) a IBM Virtual Machine Recovery Manager (VMRM DR). První dva zajišťují vysokou dostupnost v primárním DC, třetí zajišťuje funkci Disaster Recovery mezi DC.

Systémové zdroje

Pro návrh logických serverů s OS AIX je možné použít všechny poskytované druhy BB. Minimální předepsaný diskový prostor je 100 GB diskového prostoru per server.

Bezpečnost a hardening

Hardening a bezpečnostní nastavení je provedeno standardně jako součást instalace, resp. jako součást instalace patchů dle standardů Poskytovatele infrastruktury.

Patchování

Verze OS je udržována na aktuální verzi, případně na dvou předchozích uvolněných vedlejších verzích.

Instalaci patchů provádí Poskytovatel infrastruktury za součinnosti Dodavatele. Termín nasazení navrhuje Poskytovatel infrastruktury nebo Dodavatel.

3.2.2.3 Linux RedHat

Virtualizace

Pro běh logických serverů se používá:

- prostředí VMware, pokud je virtuální server provozován na platformě x64, nebo
- prostředí PowerVM, pokud je virtuální server provozován na platformě Power.

Pro Dodavatele je způsob virtualizace transparentní a nemá možnost volit mezi virtualizačními platformami konkrétní platformy.

Verze

Operační systém je aktuálně provozován ve verzi RHEL 8, RHEL 7.5 a 7.6.

Vysoká dostupnost

Vysoká dostupnost je standardně zajišťována prostředky virtualizační platformy.

Systémové zdroje

Pro návrh logických serverů s RHEL je možné použít všechny poskytované druhy BB typu BB x64 1:2, resp. specifických BB na platformě Power.

Minimální předepsaný diskový prostor je 100 GB, který je nutné zohlednit při definici požadovaných služeb.

Bezpečnost a hardening

Hardening a bezpečnostní nastavení je provedeno standardně jako součást instalace, resp. jako součást instalace patchů dle standardů Poskytovatele infrastruktury.

Patchování

Verze OS je udržována na aktuální verzi, případně na dvou předchozích uvolněných vedlejších verzích.

Instalaci patchů provádí Poskytovatel infrastruktury za součinnosti Dodavatele. Termín nasazení navrhuje Poskytovatel infrastruktury nebo Dodavatel.

3.2.3 Databáze

3.2.3.1 MS SQL Server

Verze

Databáze je aktuálně provozována ve verzi MS SQL Server 2019, MS SQL Server 2018 a MS SQL Server 2016.

Vysoká dostupnost

Vysoká dostupnost je zajišťována prostředky databáze.

Systémové zdroje

Pro návrh logických serverů s MS SQL Serverem je možné použít všechny poskytované druhy BB s OS MS Windows.

Minimální předepsaný diskový prostor je 100 GB dedikovaných pro databázi MS SQL Server.

Bezpečnost a hardening

Hardening a bezpečnostní nastavení je provedeno standardně jako součást instalace, resp. jako součást instalace patchů dle standardů Poskytovatele infrastruktury.

Šifrování nebo jiné dodatečné aplikační opatření nejsou standardně nasazována.

Patchování

Verze databáze MS SQL Server je udržována na aktuální verzi, případně na dvou předchozích uvolněných vedlejších verzích.

Instalaci patchů provádí Poskytovatel infrastruktury za součinnosti Dodavatele. Termín nasazení navrhuje Poskytovatel infrastruktury nebo Dodavatel.

Zálohování

Zálohování databáze se provádí pomocí nástroje IBM Spectrum Protect Plus (IBM SPP).

3.2.3.2 PostgreSQL

Verze

Databáze je aktuálně provozována ve verzi PostgreSQL 12.1, 11.6 a 10.11.

Vysoká dostupnost

Vysoká dostupnost je zajišťována prostředky databáze.

Systémové zdroje

Pro návrh logických serverů s databázovým serverem PostgreSQL je možné použít všechny poskytované druhy Building bloků s OS MS Windows a OS Linux RHEL.

Minimální předepsaný diskový prostor je 100 GB dedikovaných pro databázi PostgreSQL.

Bezpečnost a hardening

Hardening a bezpečnostní nastavení je provedeno standardně jako součást instalace, resp. jako součást instalace patchů dle standardů Poskytovatele infrastruktury.

Šifrování nebo jiné dodatečné aplikační opatření nejsou standardně nasazována.

Patchování

Verze databáze PostgreSQL je udržována na aktuální verzi, případně na dvou předchozích uvolněných vedlejších verzích.

Instalaci patchů provádí Poskytovatel infrastruktury za součinnosti Dodavatele. Termín nasazení navrhuje Poskytovatel infrastruktury nebo Dodavatel.

Zálohování

Zálohování databáze se provádí pomocí nástroje IBM Spectrum Protect Plus (IBM SPP).

3.3 Definice služeb infrastruktury

Následující kapitoly definuje jednotlivé infrastrukturní služby, které lze použít pro návrh technické architektury v Příloze 7 – Infrastrukturní požadavky Dodavatele.

3.3.1 Infrastrukturní služby na úrovni OS

Tabulka 5 – Infrastrukturní služby OS MS Windows 2018 Server

Platforma	Operační systém	Primární vs. Záložní DC	ID	Building Blok	vCPU	vRAM	Body
x64	Windows 2018 Server	Neredundantní	VS_X64_WIN_NR_4_1	1:4	1	4	291
			VS_X64_WIN_NR_4_2	1:4	2	8	582
			VS_X64_WIN_NR_4_4	1:4	4	16	1165
			VS_X64_WIN_NR_4_6	1:4	6	24	1748
			VS_X64_WIN_NR_4_8	1:4	8	32	2330
			VS_X64_WIN_NR_4_12	1:4	12	48	3496
			VS_X64_WIN_NR_4_16	1:4	16	64	4661
			VS_X64_WIN_NR_4_32	1:4	32	128	9322
		Redundantní	VS_X64_WIN_R_4_1	1:4	1	4	986
			VS_X64_WIN_R_4_2	1:4	2	8	1972
			VS_X64_WIN_R_4_4	1:4	4	16	3944
			VS_X64_WIN_R_4_6	1:4	6	24	5917
			VS_X64_WIN_R_4_8	1:4	8	32	7889
			VS_X64_WIN_R_4_12	1:4	12	48	11834
			VS_X64_WIN_R_4_16	1:4	16	64	15779
			VS_X64_WIN_R_4_32	1:4	32	128	31559

Příloha č. 6 Smlouvy služby infrastruktury

Tabulka 6 – Infrastrukturní služby OS RedHat Enterprise Linux na platformě x86

Platforma	Operační systém	Primární vs. Záložní DC	ID	Building Blok	vCPU	vRAM	Body
x64	RHEL	Neredundantní	VS_X64_RHEL_NR_2_1	1:2	1	2	122
			VS_X64_RHEL_NR_2_2	1:2	2	4	245
			VS_X64_RHEL_NR_2_4	1:2	4	8	490
			VS_X64_RHEL_NR_2_6	1:2	6	12	735
			VS_X64_RHEL_NR_2_8	1:2	8	16	980
			VS_X64_RHEL_NR_2_12	1:2	12	24	1470
			VS_X64_RHEL_NR_2_16	1:2	16	32	1960
			VS_X64_RHEL_NR_2_32	1:2	32	64	3920
		Redundantní	VS_X64_RHEL_R_2_1	1:2	1	2	648
			VS_X64_RHEL_R_2_2	1:2	2	4	1297
			VS_X64_RHEL_R_2_4	1:2	4	8	2594
			VS_X64_RHEL_R_2_6	1:2	6	12	3891
			VS_X64_RHEL_R_2_8	1:2	8	16	5188
			VS_X64_RHEL_R_2_12	1:2	12	24	7782
			VS_X64_RHEL_R_2_16	1:2	16	32	10376
			VS_X64_RHEL_R_2_32	1:2	32	64	20753

Příloha č. 6 Smlouvy služby infrastruktury

Tabulka 7 – Infrastrukturní služby OS RedHat Enterprise Linux na platformě Power

Platforma	Operační systém	Primární vs. Záložní DC	ID	Building Blok	CPU	RAM	Body
Power9	RHEL	Neredundantní	VS_PWR_RHEL_NR_50_02	1:50	0,2	10	14668
			VS_PWR_RHEL_NR_50_04	1:50	0,4	20	22563
			VS_PWR_RHEL_NR_50_06	1:50	0,6	30	30458
			VS_PWR_RHEL_NR_50_08	1:50	0,8	40	38352
			VS_PWR_RHEL_NR_50_1	1:50	1	50	46247
			VS_PWR_RHEL_NR_50_2	1:50	2	100	85721
			VS_PWR_RHEL_NR_50_4	1:50	4	200	164668
			VS_PWR_RHEL_NR_50_6	1:50	6	300	243616
			VS_PWR_RHEL_NR_50_8	1:50	8	400	322563
			VS_PWR_RHEL_NR_50_12	1:50	12	600	480458
		Redundantní	VS_PWR_RHEL_NR_50_16	1:50	16	800	638352
			VS_PWR_RHEL_R_50_02	1:50	0,2	10	23811
			VS_PWR_RHEL_R_50_04	1:50	0,4	20	34074
			VS_PWR_RHEL_R_50_06	1:50	0,6	30	44337
			VS_PWR_RHEL_R_50_08	1:50	0,8	40	54600
			VS_PWR_RHEL_R_50_1	1:50	1	50	64863
			VS_PWR_RHEL_R_50_2	1:50	2	100	116179
			VS_PWR_RHEL_R_50_4	1:50	4	200	218811
			VS_PWR_RHEL_R_50_6	1:50	6	300	321442
			VS_PWR_RHEL_R_50_8	1:50	8	400	424074
		Neredundantní	VS_PWR_RHEL_R_50_12	1:50	12	600	629337
			VS_PWR_RHEL_R_50_16	1:50	16	800	834600
			VS_PWR_RHEL_NR_80_02	1:80	0,2	16	18774

Příloha č. 6 Smlouvy služby infrastruktury

Platforma	Operační systém	Primární vs. Záložní DC	ID	Building Blok	CPU	RAM	Body
			VS_PWR_RHEL_NR_80_04	1:80	0,4	32	74307
			VS_PWR_RHEL_NR_80_06	1:80	0,6	48	42774
			VS_PWR_RHEL_NR_80_08	1:80	0,8	64	54774
			VS_PWR_RHEL_NR_80_1	1:80	1	80	66774
			VS_PWR_RHEL_NR_80_2	1:80	2	160	126774
			VS_PWR_RHEL_NR_80_4	1:80	4	320	246774
			VS_PWR_RHEL_NR_80_6	1:80	6	480	366774
			VS_PWR_RHEL_NR_80_8	1:80	8	640	486774
			VS_PWR_RHEL_NR_80_12	1:80	12	960	726774
			VS_PWR_RHEL_NR_80_16	1:80	16	1280	966774
			VS_PWR_RHEL_R_80_02	1:80	0,2	16	29148
			VS_PWR_RHEL_R_80_04	1:80	0,4	32	44748
			VS_PWR_RHEL_R_80_06	1:80	0,6	48	60348
			VS_PWR_RHEL_R_80_08	1:80	0,8	64	75948
			VS_PWR_RHEL_R_80_1	1:80	1	80	91548
			VS_PWR_RHEL_R_80_2	1:80	2	160	169548
Redundantní			VS_PWR_RHEL_R_80_4	1:80	4	320	325548
			VS_PWR_RHEL_R_80_6	1:80	6	480	481548
			VS_PWR_RHEL_R_80_8	1:80	8	640	637548
			VS_PWR_RHEL_R_80_12	1:80	12	960	949548
			VS_PWR_RHEL_R_80_16	1:80	16	1280	1261548

Příloha č. 6 Smlouvy služby infrastruktury

Tabulka 8 – Infrastrukturní služby OS IBM AIX

Platforma	Operační systém	Primární vs. Záložní DC	ID	Building Blok	CPU (resp. vCPU)	RAM (resp. vRAM)	Body
Power9	AIX	Neredundantní	VS_PWR_AIX_NR_50_02	1:50	0,2	10	14668
			VS_PWR_AIX_NR_50_04	1:50	0,4	20	22563
			VS_PWR_AIX_NR_50_06	1:50	0,6	30	30458
			VS_PWR_AIX_NR_50_08	1:50	0,8	40	38352
			VS_PWR_AIX_NR_50_1	1:50	1	50	46247
			VS_PWR_AIX_NR_50_2	1:50	2	100	85721
			VS_PWR_AIX_NR_50_4	1:50	4	200	164668
			VS_PWR_AIX_NR_50_6	1:50	6	300	243616
		Redundantní	VS_PWR_AIX_NR_50_8	1:50	8	400	322563
			VS_PWR_AIX_NR_50_12	1:50	12	600	480458
			VS_PWR_AIX_NR_50_16	1:50	16	800	638352
			VS_PWR_AIX_R_50_02	1:50	0,2	10	23811
			VS_PWR_AIX_R_50_04	1:50	0,4	20	34074
			VS_PWR_AIX_R_50_06	1:50	0,6	30	44337
			VS_PWR_AIX_R_50_08	1:50	0,8	40	54600
			VS_PWR_AIX_R_50_1	1:50	1	50	64863
			VS_PWR_AIX_R_50_2	1:50	2	100	116179
			VS_PWR_AIX_R_50_4	1:50	4	200	218811
			VS_PWR_AIX_R_50_6	1:50	6	300	321442
			VS_PWR_AIX_R_50_8	1:50	8	400	424074
			VS_PWR_AIX_R_50_12	1:50	12	600	629337
			VS_PWR_AIX_R_50_16	1:50	16	800	834600

- Aplikační infrastrukturní služby

Příloha č. 6 Smlouvy služby infrastruktury

Tabulka 9 – Infrastrukturní služby MS SQL 2016 Server

Platforma	Operační systém	Aplikace	Primární vs. Záložní DC	ID	Building Blok	vCPU	vRAM	Body
x64	Windows 2018 Server	MS SQL Server	Neredundantní	VS_X64_WIN_MSS_NR_4_2	1:4	2	8	15433
				VS_X64_WIN_MSS_NR_4_4	1:4	4	16	16015
				VS_X64_WIN_MSS_NR_4_6	1:4	6	24	16598
				VS_X64_WIN_MSS_NR_4_8	1:4	8	32	17181
				VS_X64_WIN_MSS_NR_4_12	1:4	12	48	18346
				VS_X64_WIN_MSS_NR_4_16	1:4	16	64	19511
				VS_X64_WIN_MSS_NR_4_32	1:4	32	128	24173
				VS_X64_WIN_MSS_R_4_2	1:4	2	8	31673
			Redundantní	VS_X64_WIN_MSS_R_4_4	1:4	4	16	33645
				VS_X64_WIN_MSS_R_4_6	1:4	6	24	35618
				VS_X64_WIN_MSS_R_4_8	1:4	8	32	37590
				VS_X64_WIN_MSS_R_4_12	1:4	12	48	41535
				VS_X64_WIN_MSS_R_4_16	1:4	16	64	45480
				VS_X64_WIN_MSS_R_4_32	1:4	32	128	61260
			Redundantní	VS_PWR_AIX_ORA_NR_50_8	1:50	8	400	330853
				VS_PWR_AIX_ORA_NR_50_12	1:50	12	600	488748
				VS_PWR_AIX_ORA_NR_50_16	1:50	16	800	646643
				VS_PWR_AIX_ORA_R_50_06	1:50	0,6	30	60918
				VS_PWR_AIX_ORA_R_50_08	1:50	0,8	40	71181
				VS_PWR_AIX_ORA_R_50_1	1:50	1	50	81444
				VS_PWR_AIX_ORA_R_50_2	1:50	2	100	132760
				VS_PWR_AIX_ORA_R_50_4	1:50	4	200	235391

Příloha č. 6 Smlouvy služby infrastruktury

Platforma	Operační systém	Aplikace	Primární vs. Záložní DC	ID	Building Blok	vCPU	vRAM	Body
				VS_PWR_AIX_ORA_R_50_6	1:50	6	300	338023
				VS_PWR_AIX_ORA_R_50_8	1:50	8	400	440654
				VS_PWR_AIX_ORA_R_50_12	1:50	12	600	645918
				VS_PWR_AIX_ORA_R_50_16	1:50	16	800	851181

Příloha č. 6 Smlouvy služby infrastruktury

Tabulka 10 – Infrastrukturní služby PostgreSQL Server

Platforma	Operační systém	Aplikace	Primární vs. Záložní DC	ID	Building Blok	vCPU	vRAM	Body
x64	Windows 2018 Server	PostgreSQL	Neredundantní	VS_X64_WIN_PGR_NR_4_4	1:4	4	16	16015
				VS_X64_WIN_PGR_NR_4_6	1:4	6	24	16598
				VS_X64_WIN_PGR_NR_4_8	1:4	8	32	17181
				VS_X64_WIN_PGR_NR_4_12	1:4	12	48	18346
			VS_X64_WIN_PGR_NR_4_16	1:4	16	64	19511	
			VS_X64_WIN_PGR_NR_4_32	1:4	32	128	24173	
			VS_X64_WIN_PGR_R_4_4	1:4	4	16	33645	
			VS_X64_WIN_PGR_R_4_6	1:4	6	24	35618	
	Redundantní		VS_X64_WIN_PGR_R_4_8	1:4	8	32	37590	
			VS_X64_WIN_PGR_R_4_12	1:4	12	48	41535	
			VS_X64_WIN_PGR_R_4_16	1:4	16	64	45480	
			VS_X64_WIN_PGR_R_4_32	1:4	32	128	61260	
			VS_X64_RHEL_PGR_NR_2_4	1:2	4	8	15554	
			VS_X64_RHEL_PGR_NR_2_6	1:2	6	12	15799	
			VS_X64_RHEL_PGR_NR_2_8	1:2	8	16	16044	
			VS_X64_RHEL_PGR_NR_2_12	1:2	12	24	16534	
RHEL	VS_X64_RHEL_PGR_NR_2_16	1:2	16	32	17024			
	VS_X64_RHEL_PGR_NR_2_32	1:2	32	64	18984			
	VS_X64_RHEL_PGR_R_2_4	1:2	4	8	32722			
	VS_X64_RHEL_PGR_R_2_6	1:2	6	12	34019			
	VS_X64_RHEL_PGR_R_2_8	1:2	8	16	35317			
	VS_X64_RHEL_PGR_R_2_12	1:2	12	24	37911			
	VS_X64_RHEL_PGR_R_2_16	1:2	16	32	40505			

Platforma	Operační systém	Aplikace	Primární vs. Záložní DC	ID	Building Blok	vCPU	vRAM	Body
				VS_X64_RHEL_PGR_R_2_32	1:2	32	64	50882

3.3.2 Diskové infrastrukturní služby

Tabulka 11 – Infrastrukturní služby Diskový prostor

Platforma	Primární vs. Záložní DC	ID	Jednotka	Body
Diskový prostor	Neredundantní	STOR1	GB	3,23
	Redundantní	STOR1	GB	6,91
	Neredundantní	STOR3	GB	2,4

4 Průřezové služby infrastruktury

Tato kapitola popisuje průřezové služby infrastruktury, které poskytují technické nebo aplikační funkcionality obvykle nezbytné pro definici architektury implementovaného řešení.

Služby jsou součástí služeb DC a pokud budou Dodavatelem použité v souladu s jejich definicí, není je třeba uvádět v seznamu použitých služeb v Příloze 7 – Infrastrukturní požadavky Dodavatele.

4.1 DNS

Služby DNS jsou poskytovány automaticky pro všechny rozsahy adresy, přístupné z externích prostředí (internet, CMS2, GOVBONE, interní síť MF).

Pro interní komunikaci v rámci navrhovaného řešení je třeba zajistit nastavení na úrovni příslušného OS (hosts), případně nastavení DNS služby v rámci aplikace.

4.2 NFS

Služby NFS nejsou centrálně poskytovány, případné sdílení filesystémů v rámci řešení je nutné řešit jako součást dodávané architektury aplikace prostředky příslušného OS nebo jako součást aplikace (tj. např. NFS služba, SAMBA, FreeNAS a podobně).

4.3 DHCP

V rámci DC jsou poskytovány výhradně služby provozu serverových řešení, kterým jsou přidělovány pevné adresy z rozsahů definovaných Poskytovatelem infrastruktury. Služby dynamického přidělování adres tedy nejsou poskytovány.

Výjimkou jsou služby kontejnerizace, kde je adresa přidělena jako součást parametrů kontejneru při jeho spuštění.

4.4 Mailové služby

Mailové služby jsou poskytovány ve formě SMTP serveru, výhradně pro odchozí mailovou komunikaci (notifikace).

4.5 VPN

Služby VPN jsou poskytovány v rámci služeb DC Poskytovatele infrastruktury výhradně pro potřeby vzdálené administrace, zpravidla pro potřeby Dodavatele, a to jak pro fázi implementací, tak pro fázi provozní podpory.

Součástí služby je vytvoření specifické skupiny uživatelů Dodavatele, která zajišťuje oprávnění přístupu ke službám, které jsou součástí služeb řešení. Skupina VPN klientů není vnitřně diverzifikovaná.

4.6 LoadBalancing

Jako součást služeb DC je možné při návrhu řešení využít služeb LoadBalancingu. LoadBalancing je zajišťován na úrovni síťové infrastruktury a poskytuje jednoduchý round-robin balancing nad protokoly HTTP a HTTPS.

4.7 Firewall

Zabezpečení je realizované pomocí firewallových pravidel. Veškerá síťová komunikace podléhá pravidlům pro komunikaci.

Aplikace, resp. řešení Dodavatele musí být navržena s ohledem na možnost monitorovat, resp. řídit komunikaci. Základním předpokladem je rozvrstvení aplikace do vrstev (segmentů), které mají společné vlastnosti, požadavky na infrastrukturu, monitoring nebo procesy podpory. Optimálně je pro návrh aplikace využito rozdělení na tyto vrstvy:

- databázová vrstva, která je zodpovědná za persistenci dat;
- aplikační vrstva, která je zodpovědná za procesní a funkční zpracování dat;
- vrstva uživatelského rozhraní, které je zodpovědné za poskytnutí uživatelského rozhraní;
- pro návrh řešení a síťového prostředí pak platí následující pravidla:
 - veškerá komunikace (tedy externí i interní, tedy mezi komponentami řešení) musí být šifrovaná;
 - komunikace mezi vrstvami (segmenty) je kontrolována firewalllem, v rámci vrstvy (segmentu) neprochází kontrolou firewallu;
 - komunikace s externím prostředím (internet, GOVBONE) musí procházet přes aplikační firewall F5.

4.8 Proxy

Služby proxy serveru, stejně jako služby reverzní proxy, nejsou centrálně poskytovány.

Pokud jsou tyto služby vyžadovány, musí být zabezpečeny jako součást řešení (např. s využitím služeb OS).

4.9 ServiceDesk

Služba poskytuje podporu uživatelům podporu činností spojených s evidencí a řešením servisního hlášení včetně základní klasifikace (zařazení do správné kategorie). SD zajišťuje v rámci životního cyklu servisního hlášení automatickou (e-mailovou) notifikaci osob, spojených s daným servisním hlášením (řešitelé, koncový uživatel, operátoři SD). Nad každým servisním hlášením probíhá měření plnění SLA (dle jeho kategorie) a je zajištěna eskalace (e-mail + telefonát operátora) v případě hrozícího porušení SLA.

O vyřešení servisního hlášení je uživatel automaticky informován. V případě závažnějšího problému operátor SD zajistí předání servisního hlášení na příslušnou řešitelskou skupinu další úrovně podpory.

Využívány jsou všechny typy kategorií servisních hlášení dle metodiky ITIL, tedy požadavky na podporu, požadavky na informaci, požadavky na změnu a hlášení poruchy (incidentu).

4.10 Provozní dohled

Služba poskytuje monitoring infrastruktury DC, sítí, HW, operačních systémů, databází a aplikací. Zajišťuje sběr událostí v jednotlivých vrstvách a částech systémů, které by mohly mít vliv na správný chod aplikací v případě výskytu definované odchylky od standardních požadovaných hodnot.

4.11 Bezpečnostní monitoring

Bezpečnostní monitoring je součástí standardních služeb poskytovaných v rámci provozu DC Poskytovatele infrastruktury.

Vzhledem k tomu, že vybrané IS Objednatele provozované jako součást sdílené infrastruktury musí splňovat požadavky na významný IS nebo Kritickou informační infrastrukturu dle zákona č. 181/2014 Sb., zavazuje se obecně Dodavatel dodržovat relevantní ustanovení zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících předpisů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). Dodavatel je povinen v souladu s požadavky vyhlášky č. 82/2018 Sb. a ve vzájemně odsouhlaseném rozsahu dodržovat následující pravidla:

- nakládat s daty v souladu s jejich účelem a dodržovat pravidla pro likvidaci dat;
- dodržovat bezpečnostní politiky a bezpečnostní opatření ve formě organizačních a technických opatření;
- komunikovat o bezpečnostních událostech a incidentech;
- řídit bezpečnostní rizika;
- řídit kontinuitu provozu;
- předávat předem dohodnutou formou data, provozní údaje a informace vyžádané Objednatelem, resp. Poskytovatelem infrastruktury.

4.12 Testy

Součástí podpory provozu jsou pravidelné testy prostředí. Jejich předmětem jsou zejména testy zajištění kontinuity služeb (Disaster recovery), ale také ad-hoc testy technických zařízení a programového vybavení (např. při upgradu/updatu jednotlivých vrstev aplikace).

Řešení včetně příslušných procesů musí být schopné zajistit pravidelné testování, a to na příslušném prostředí. Obvykle se využívá následující rozdělení:

- testovací prostředí je využíváno pro testování DR procesů a postupů a pro testy aplikací (rozvoj, upgrade, update) na všech vrstvách architektury,

- produkční prostředí prochází minimálně 1x ročně DR testy s ověřením provozu v záložní lokalitě (je-li pro řešení vyžadovaná tato konfigurace).

Tyto testy nevylučují ani neomezují aplikační testy, definované v popisu funkčních požadavků v Příloze 1 - Funkční a technické požadavky.

Tyto testy musí být provedeny v rámci produkčního prostředí před přechodem řešení do produktivního provozu.

5 Architektonické principy

5.1 Pravidla pro návrh architektury řešení

5.1.1 Adaptabilita a flexibilita

IS jsou investice, které si Objednatel pořizuje s cílem zajistit požadované funkcionality a procesy, a to s výhledem na řadu let provozu. Zároveň obvykle řešení prochází během svého životního cyklu (a často i během implementace) řadou změn, kdy je nutné reagovat na změny podmínek, požadavků nebo technických komponent. Řešení tedy musí být navrhované takovým způsobem, aby bylo flexibilní a umožnilo Objednateli pružně reagovat na výzvy během produktivního provozu aplikace. Předpokladem je minimálně splnění následujících podmínek:

- návrh řešení bez vytvoření závislosti na jednom dodavateli (vendor-lock);
- veškerá (nevýhradní) práva a zdrojové kódy jsou součástí plnění a přecházejí na objednatele;
- pokud je to možné, jsou implementované procesy a funkcionality řešeny tak, aby byly bez vazby na konkrétní technologie;
- maximální podpora virtualizace a virtuálního datového centra, bez úzké vazby na HW platformu;
- využívání otevřených řešení, u kterých je zaručena dlouhodobá stabilita při podpoře a dalším rozvoji;
- podpora flexibilního prostředí s maximálně možnou dynamikou;
- preference technologií s možností několika alternativních dodavatelů nebo implementátorů.

5.1.2 Standardizace procesů rozvoje a podpory

Standardizace procesů administrace, podpory a správy softwaru je základním předpokladem pro úspěšný a bezproblémový chod IS. Navrhované řešení musí podporovat standardní nástroje pro tyto oblasti a zajistit podporu procesům spojených s provozem celého řešení.

- preferována je 3 vrstvá architektura s oddělením databázové, aplikační a prezentační vrstvy;

- celkové řešení architektury a procesů podpory zahrnuje oddělené produkční a neprodukční prostředí, obvykle ještě dále členěné na oddělené vývojové a testovací prostředí;
- topologie a architektura produkčního a testovacího prostředí musí být identická, odlišovat se může v sizingu testovacího prostředí;
- řešení je řádně dokumentované a případné zdrojové kódy (scripty) jsou verzovány a předávány do interního prostředí GitLab včetně všech souvisejících konfiguračních údajů. Stejně pravidlo se vztahuje i na veškeré pomocné aplikační vybavení, které není samo není předmětem řešení IS, které ale Dodavatel při jeho vývoji, testování, nasazení a správě využívá;
- návrh prostředí a zvolené technologie odpovídají aktuálním trendům IT;
- součástí dodávky IS musí být i návrh zapojení administrace a podpory provozu do standardních procesů správy IT Objednatele, resp. Poskytovatele infrastruktury.

5.1.3 Bezpečnost

Bezpečnost vnímáme jako klíčovou součást navrženého řešení pro zajištění privátnosti a integrity informací. Z hlediska architektury bude návrh zahrnovat především vytvoření takové infrastruktury, která dokáže dostatečně pružně reagovat na požadavky bezpečnostní politiky. Cílem je nejen dodržení všech zákonných norem platných v této oblasti, ale také zajištění důvěryhodnosti celého systému.

Řešení musí zajistit všechna bezpečnostní opatření, relevantní kvalitě a citlivosti dat, která zpracovává. Součástí implementačního procesu musí být také klasifikace dat a navržení technických i procesních opatření k jejich ochraně.

5.1.4 Náklady na vlastnictví a provoz

Řešení musí zohlednit, zejména z dlouhodobého hlediska, cenově nejpříznivější variantu (samozřejmě s ohledem na zajištění požadovaných procesů a funkcionalit). Při návrhu musí být respektován nejen výchozí a požadovaný stav, ale také náročnost údržby a obnovy. Preferovány jsou takové alternativy architektury, které zajistí minimalizaci rozsahu používaných technologií, usnadní správu technologického portfolia a umožní opakování ověřených jednoduchých návrhových vzorů.

Řešení také musí zajistit bezproblémový chod ve virtualizovaném prostředí a v cloudu, které umožní Objednateli volit optimální model provozu řešení.

Cílem je dosažení co nejnižších celkových nákladů na vlastnictví (TCO).

5.1.5 Dokumentace

Dokumentace řešení ve všech fázích projektu je definovaná v Příloze 1 - Funkční a technické požadavky a v Příloze 2 - Požadavky na dokumentaci.

5.2 Základní rysy architektury

Navrhovaná architektura musí splňovat následující požadavky a vlastnosti.

5.2.1 Škálovatelnost

Navrhovaná architektura bude schopna pokrýt vzrůstající počet uživatelů, funkcionalit a dat, spravovaných v rámci systému. Škálovatelnost se v tomto smyslu netýká jen růstu počtu uživatelů a množství dat, resp. požadavku na výpočetní výkon, ale i možnosti nasazení distribuovaných aplikací. Cílem je architektura, která neobsahuje úzká místa a dovolí růst od malých nebo pilotních řešení ke komplexnímu celostátnímu nasazení.

5.2.2 Dostupnost

Zajištění kontinuity služeb, a tedy vysoké dostupnosti je základním předpokladem provozu většiny moderních IS. Způsobů zajištění je celá řada a záleží na Dodavateli, aby kombinací vhodných aplikačních funkcí a služeb infrastruktury navrhl řešení, které bude splňovat parametry a kritéria požadovaná zadávací dokumentací.

Architektura bude důsledně respektovat požadavky na potřebnou dostupnost klíčových komponent. Řešení v tomto případě zahrnuje nejen vhodně volené prostředky IT, ale také určení procesů a prostředků údržby, zálohování, krizových procesů aj. Cílem je zajistit kontinuitu procesů a služeb směrem ke koncovým uživatelům.

5.2.3 Monitorování a varování

Bez mechanismů monitorování a varování je nemožné udržet dostupnost prostředí. Je naprosto nezbytné, aby byl správce systému okamžitě informován (např. formou upozornění – alertů) o jakémkoliv selhání tak, aby jej mohl co nejrychleji napravit. Monitorování a varování je také klíčové pro bezpečnostní strategii. Navržená architektura musí splňovat požadavek na vysokou úroveň kontroly (auditování) důležitých oblastí systému a procesů a událostí v systému probíhajících.

5.2.4 Zálohování a obnova

Součástí navrženého řešení bude integrace na centrální systém pro zálohování a obnovu dat. Řešení bude obsahovat podrobné postupy pro zálohování a obnovu každé komponenty řešení, stejně jako plán obnovy celkové architektury řešení s ohledem na používaný zálohovací software.

5.3 Preferované architektonické patterny

Tato kapitola popisuje základní doporučené přístupy k návrhu technické architektury a jejího začlenění do prostředí DC Provozovatele infrastruktury.

5.3.1 Samostatný virtuální server

Předpoklady

Předpoklady architektury samostatného virtuálního serveru:

- základní, nereplikované virtuální servery;

- dostupné všechny typy diskových služeb (STOR1 i STOR3);
- dostupné všechny služby jednoho (obvykle Primárního) DC;
- přístup uživatele je povolen s ohledem na zvolené a schválené politiky konektivity;
- přístup Administrátora je povolen prostřednictvím VPN na úroveň virtuálního serveru.

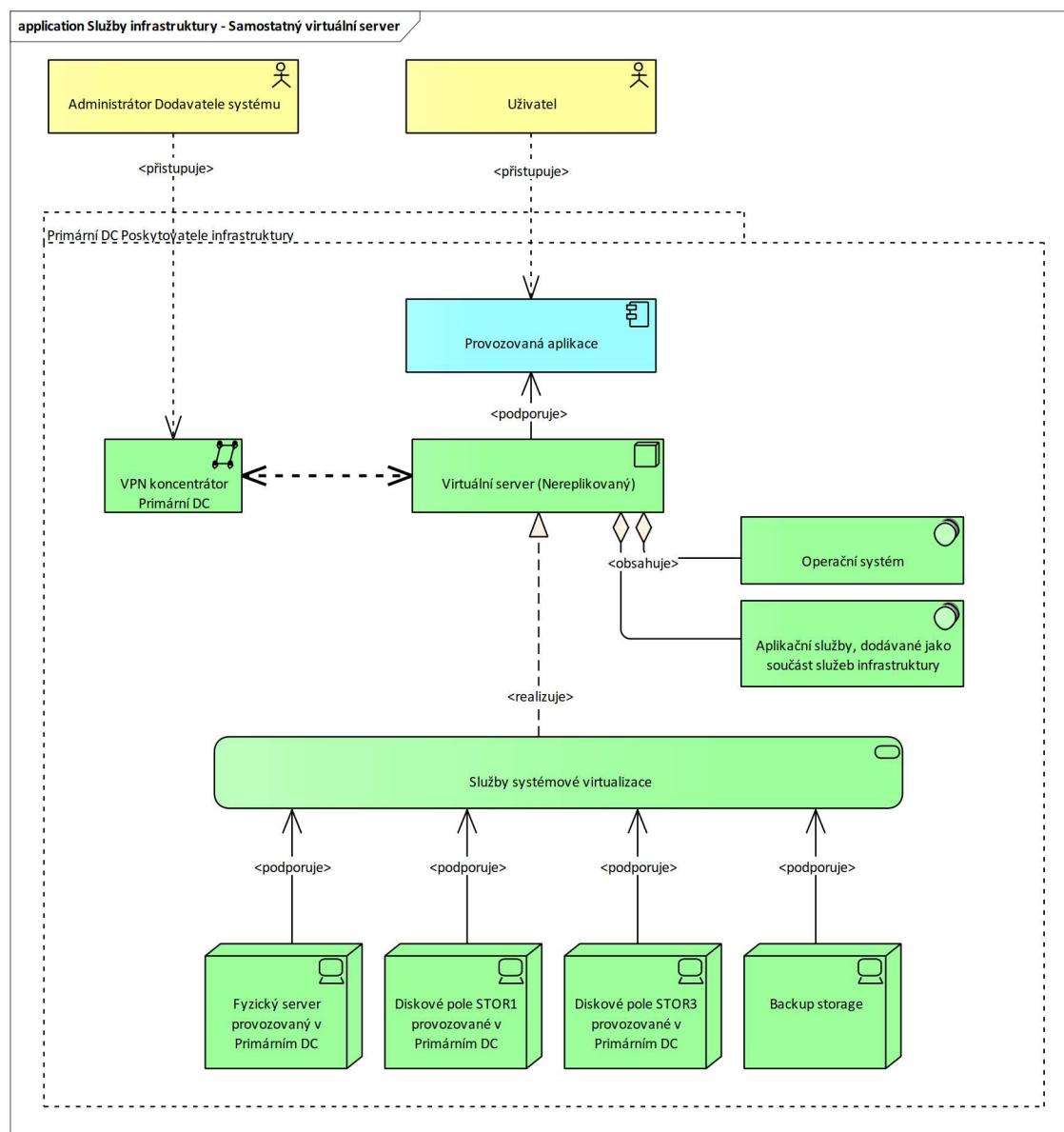
Popis architektury

Pattern je založen na využití nereplikovaných virtuálních serverů, které jsou provozovány vždy v jednom (obvykle Primárním) DC.

Umístění virtuálního serveru (tedy to, v jakém DC je virtuální server provozován) nemá vliv na jeho konektivitu nebo na dostupnost průřezových služeb infrastruktury. Stejně tak dostupnost zálohovacích technologií je transparentní a nezávisí na DC, ve kterém je virtuální server provozován (nezávisle na tom, zda se jedná o backup nebo restore).

Vysoká dostupnost je založena na službách příslušné virtualizační platformy. Pokud je to možné, virtuální server je automaticky zprovozněn v DC, ve kterém je provozován v rámci garantované SLA. Poskytovatel infrastruktury garantuje přístupnost funkcionalit, které jsou součástí služby infrastruktury. Dostupnost aplikačních služeb garantuje Dodavatel.

Příloha č. 6 Smlouvy služby infrastruktury



Obrázek 1 Služby infrastruktury – samostatný virtuální server

5.3.2 Vysoká dostupnost mezi datovými centry

Předpoklady

Předpoklady architektury virtuálního serveru replikovaného přes 2 datová centra:

- využití replikovaných virtuálních serverů;
 - diskové služby kategorie STOR1. Datový obsah je replikován:
 - synchronně na úrovni diskového pole (pro platformu Power);
 - asynchronně prostředky VMware (pro platformu x64)
- v závislosti na použité virtualizační platformě,

- přístup uživatele je povolen s ohledem na zvolené a schválené politiky konektivity. Doporučuje se použití služeb Load Balanceru (buď dostupné služby infrastruktury, nebo jako vlastnost nasazované aplikace);
- přístup Administrátora je povolen prostřednictvím VPN na úroveň virtuálního serveru, a to do obou DC (samozřejmě že v Záložním DC je server dostupný po jeho převedení a aktivaci);
- pro návrh infrastruktury jsou dostupné všechny služby obou DC.

Popis architektury

Pattern je založen na využití replikovaných virtuálních serverů, přičemž standardně je virtuální server provozován v Primárním DC. V Záložním DC je alokován příslušný výpočetní výkon, ovšem standardně není využíván (nic na něm neběží). Data jsou replikována prostředky diskového pole (služba STOR1), přičemž replikace probíhá:

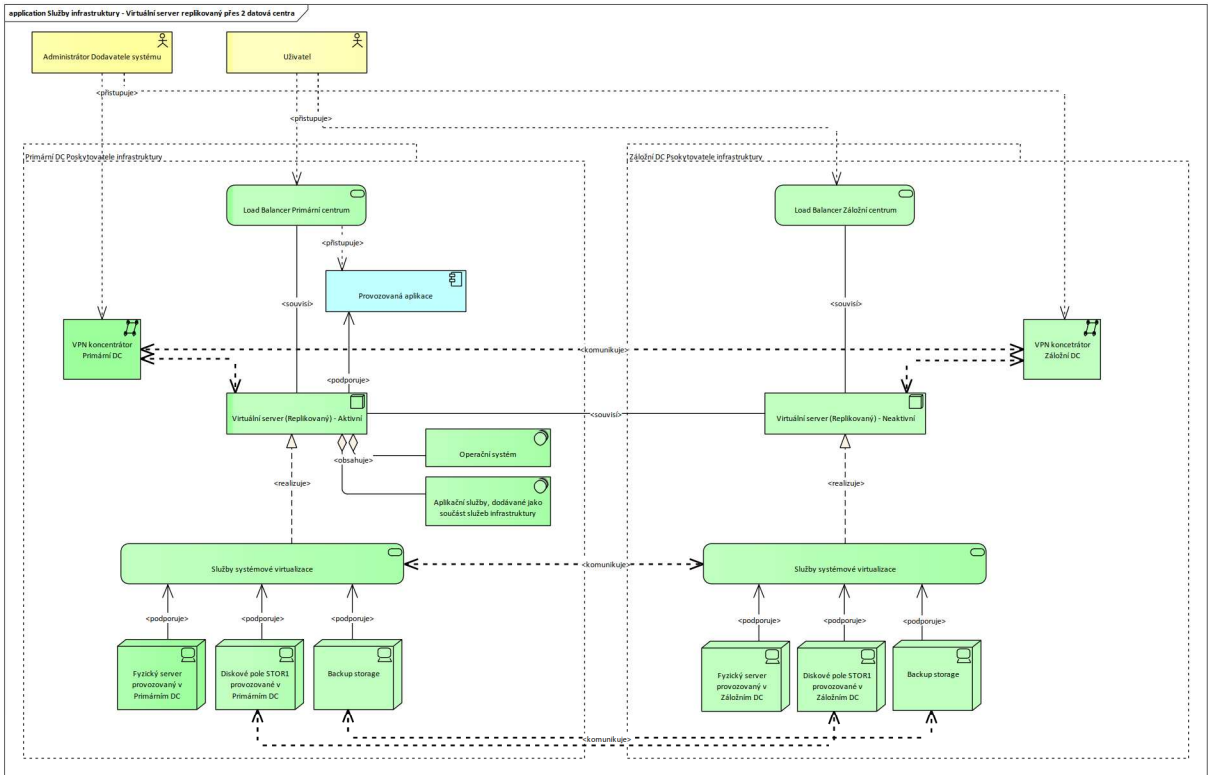
- synchronně pro virtualizační platformu Power VM (Power);
- asynchronně pro virtualizační platformu VMware (x64).

Umístění virtuálního serveru (tedy to, v jakém DC v konkrétním okamžiku běží virtuální server) nemá vliv na jeho konektivitu nebo na dostupnost průřezových služeb infrastruktury. Stejně tak dostupnost zálohovacích technologií je transparentní a nezávisí na DC, ve kterém je virtuální server v daném okamžiku provozován (nezávisle na tom, zda se jedná o backup nebo restore).

Vysoká dostupnost je založena na službách příslušné virtualizační platformy. Pokud je to možné, je virtuální server automaticky zprovozněn v Primárním DC. Pokud je Primární DC, nebo část jeho infrastruktury nedostupná, je virtuální server zprovozněn v Záložním DC. To je provedeno automaticky virtualizační platformou na základě rozhodnutí operátora.

Poskytovatel infrastruktury garantuje přístupnost funkcionalit, které jsou součástí služby infrastruktury. Dostupnost aplikačních služeb garantuje Dodavatel.

Příloha č. 6 Smlouvy služby infrastruktury



Obrázek 2 Služby infrastruktury – virtuální server replikovaný