Technická specifikace řešení pro zajištění maximální dostupnosti aplikace Vitakarta

1 AKTUÁLNÍ STAV

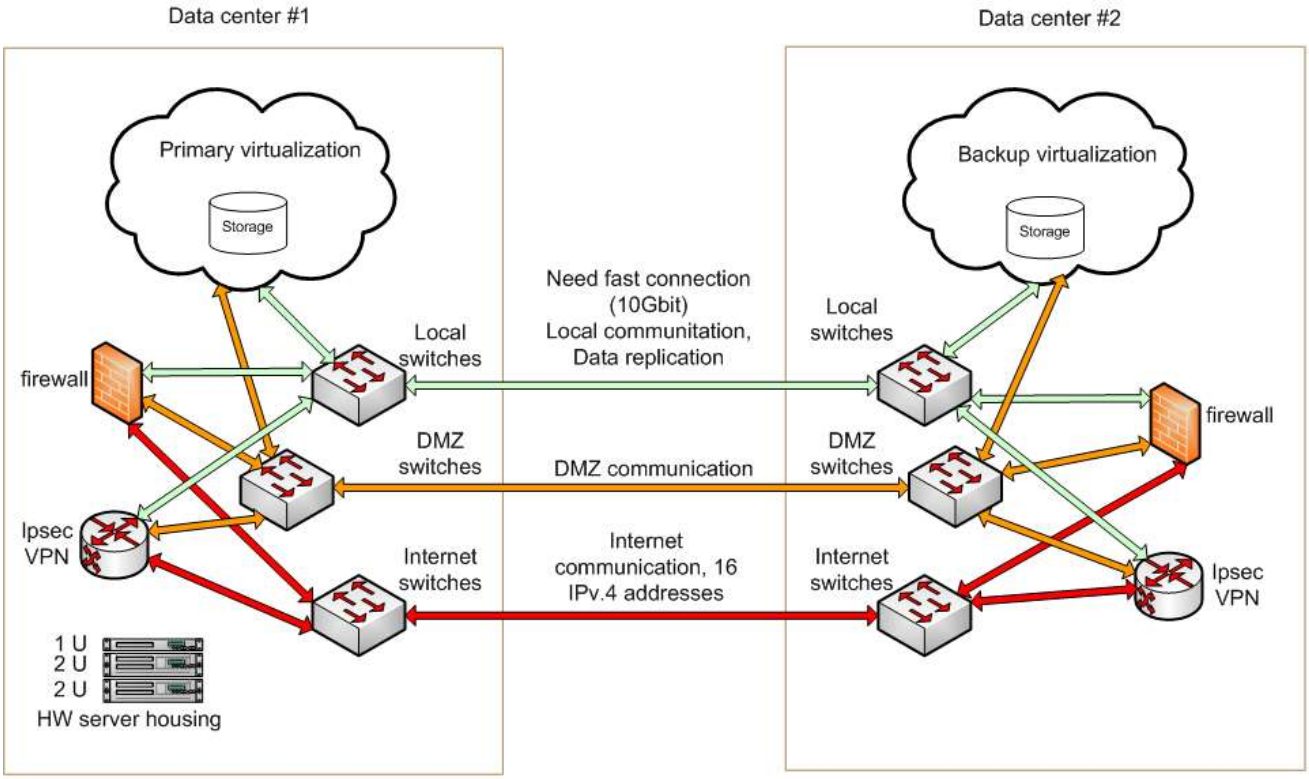
Datové centrum momentálně zajišťuje následující služby bez redundantního záložního systému:

- Správu a pronájem prostředků pro provozování virtuálních serverů, na kterých běží servery aplikace Vitakarta (VMware)
- Správu a pronájem HW prostředků, nutných k oddělenému a bezpečnému provozování sítí použitých v aplikaci Vitakarta (Internet, DMZ, localnet, testnet).
- Oddělení bezpečnostních domén je řešeno minimálně na úrovni plně stavového firewallu.
- Správu a pronájem IT prostředků pro vytvoření VPN tunelů mezi datovým centrem, OZP, a jednotlivými subUchazeči aplikace Vitakarta přes Internetové připojení.
- Vlastní aplikace běží v produkčním prostředí a druhá oddělená infrastruktura je určena pro testovací a vývojové účely.

2 CÍLOVÝ STAV

Redundantní řešení pro zajištění maximální odolnost proti výpadku aplikace Vitakarta zahrnuje.

- Redundantní řešení datového centra s kompletní replikací dat produkčního prostředí do druhé lokality.
- Redundantní spojení mezi OZP Roškotova a datovými centry prostřednictvím ISP připojení na obou stranách.



3 POŽADAVKY NA CÍLOVÉ ŘEŠENÍ REDUNDANTNÍHO DATOVÉHO CENTRA

Definice požadavku	Splněno Ano/Ne	Způsob splnění
Pro každé datové centrum dvě napájecí větve (různé fáze) s odolností vůči výpadku napájení (UPS, motor generátor) odpovídající TIER 3+.	**Ano**	Naše služby poskytujeme v následujících datových centrech, které splňují požadavky zadavatele: https://www.cra.cz/datove-centrum-dc-tower https://ttc-teleport.cz/datova-centra/ http://www.cloud4com.com/cloud4com/upload/File/c4c-technicka-specifikace-sluzeb.pdf
Vybavení každého datového centra automatickým hasicím systémem.	**Ano**	Naše služby poskytujeme v následujících datových centrech, které splňují požadavky zadavatele: https://www.cra.cz/datove-centrum-dc-tower https://ttc-teleport.cz/datova-centra/ http://www.cloud4com.com/cloud4com/upload/File/c4c-technicka-specifikace-sluzeb.pdf
Vybavení každého datového centra odpovídajícím systémem ventilace a klimatizace odpovídající TIER 3+.	**Ano**	Naše služby poskytujeme v následujících datových centrech, které splňují požadavky zadavatele: https://www.cra.cz/datove-centrum-dc-tower https://ttc-teleport.cz/datova-centra/ http://www.cloud4com.com/cloud4com/upload/File/c4c-technicka-specifikace-sluzeb.pdf
Pro každé datové centrum vytvoření a správa 3 bezpečnostních domén (Internet, DMZ a LOCAL), navzájem oddělených minimálně plně dedikovanými stavovými firewally.	**Ano**	Součástí řešení je Firewall FortiGate-VM00 Advanced Threat Protection (24x7 FortiCare plus Application Control, IPS, AV and FortiSandbox Cloud) v režimu Active-Passive zahrnující správu v rozsahu 0.5 MD za měsíc.
Prostup mezi doménou Internet a LOCAL zabezpečený oddělením přes proxy server nebo firewall s plnou inspekcí na 7 vrstvě ISO OSI modelu.	**Ano**	Součástí řešení je Firewall FortiGate-VM00 Advanced Threat Protection (24x7 FortiCare plus Application Control, IPS, AV and FortiSandbox Cloud) v režimu Active-Passive zahrnující správu v rozsahu 0.5 MD za měsíc.
Nezávislé propojení bezpečnostních domén mezi datovými centry s následujícími parametry min. 10Gbit/s služby propojení datových center.	**Ano**	Propojení uvedených datových center je realizováno minimálně dvěma nezávislými 10Gbps spoji.
Minimálně 16 veřejně routovatelných a přenositelných IP adres (v.4) pro připojení do internetu dostupných v obou datových centrech + plná podpora pro IPv6 do Internetu.	**Ano**	Součástí nabídky je celkem 16 veřejně routovatelných a přenositelných IPv4 adres dostupných v obou uvedených datových centrech.
Přistup do Internetu realizovaný minimálně dvěma redundantními navzájem nezávislými přípojkami 10Gbit/s v každém DC.	**Ano**	Přístup do Internetu je realizovaný prostřednictvím tří nezávislých spojů v každém uvedeném datovém centru o kapacitě 10 Gbps.
Pronájem a správa HW a SW prostředků pro zajištění provozních a bezpečnostních požadavků aplikace Vitakarta.	**Ano**	Součástí nabídky je pronájem a plná správa požadovaných HW a SW prostředků.
Virtuální servery nesmí být připojeny přímo do Internetu.	**Ano**	Virtuální servery jsou připojeny do interních sítí dle požadavku zadavatele. Přístup do Internetu je realizovaný pomocí dedikovaného firewallu FortiGate-VM00.
Přístup do internetu pro virtuální servery z DMZ domény musí být zajištěný minimálně plně stavovým firewallem.	**Ano**	Přístup do internetu pro virtuální servery z DMZ sítě/sítí je zajištěný pomocí dedikovaného plně stavového firewallu FortiGate-VM00.

Definice požadavku	Splněno Ano/Ne	Způsob splnění
Přístup do Internetu pro virtuální servery z LOCAL musí být zcela oddělen prostřednictvím proxy serveru, případně firewallem s plnou inspekcí na 7 vrstvě ISO OSI modelu.	**Ano**	Přístup do internetu pro virtuální servery z LOCAL sítě/sítí je zcela oddělen pomocí dedikovaného plně stavového firewallu FortiGate-VM00 s inspekcí na 7 vrstvě ISO OSI modelu.
Infrastruktura musí být schopna poskytnout tzv. SPAN port (zrcadlení veškerého definovaného provozu na fyzický port) pro monitoring a sledování bezpečnostních incidentů.	**Ano**	Nabízená infrastruktura podporuje tzv. SPAN port (zrcadlení veškerého definovaného provozu na fyzický port) pro monitoring a sledování bezpečnostních incidentů.
Automatický systém zálohování s minimální periodou pro zálohy 1 den pro primární i záložní datové centrum. Min 1x Full Backup/den Min 4x Incr/den doba obnovy dat RTO do 4 hodin doba uchování záloh min 1 měsíc uchování kopie záloh ve vzdálené lokalitě	**Ano**	Zálohování je řešeno pomocí SW Veeam Backup & Replication s plnou podporou požadovaných zálohovacích politik a uložení kopie záloh ve vzdálené lokalitě.
V případě výpadku primárního centra je záložní centrum schopno převzít produkční funkce aplikace Vitakarta do 4h (RTO max. = 4h) – požadavek pro DR. (redundantní infrastruktura bude postavena i v 2. DC)	**Ano**	Díky plné zastupitelnosti nabízené infrastruktury v záložním datovém centru je možné splnit požadavek na RTO max. = 4h pro DR. Všechny produkční virtuální servery jsou replikovány pomocí SW Veeam Backup & Replication.
Náběh záložního datového centra musí být konfigurován tak, aby nevyžadoval žádnou nebo minimální součinnost subjektů podílejících se na aplikaci Vitakarta. Primární datové centrum musí být v HA režimu, odolné proti jakémukoliv výpadku jednotlivého HW prvku.	**Ano**	Náběh záložního datového centra je konfigurován s minimální požadovanou součinností subjektů podílejících se na aplikaci Vitakarta. Infrastruktura Primárního datového centra je provozována v HA režimu (HA cluster 2 ESXi hostů), odolné proti jakémukoliv výpadku jednotlivého HW prvku.
HA řešení pro odolnost proti jakémukoliv jednotlivému výpadku není požadováno pro záložní datové centrum.	**Ano**	Z záložním datovém centru je provozován jeden ESXi host.
Záložní datové centrum nezávislé na hlavním datovém centru a to minimálně v rozsahu geografického oddělení z hlediska prostorů. Minimální vzdálenost nesmí být menší než 5 km.	**Ano**	Naše služby poskytujeme v následujících datových centrech, které splňují požadavky zadavatele: https://www.cra.cz/datove-centrum-dc-tower https://ttc-teleport.cz/datova-centra/
Aplikačně transparentní technologie pro šifrování dat v operačním systému s externím Key Management Serverem (KMS) s umístěním v lokalitě OZP.	**Ano**	Naše služba řešení s transparentním šifrováním dat v operačním systému s externím Key Management Serverem (KMS) s umístěním v lokalitě OZP podporuje díky technologii Thales (Gemalto) KeySecure a ProtectV. Služba není předmětem cenové kalkulace a je možné ji nacenit zvlášť dle požadavku zadavatele.
Připojení datových center s OZP a subUchazeči zajištěné prostřednictvím IPsec VPN se samostatnou větví pro provozní prostředí a samostatnou větví pro testovací a vývojové prostředí.	**Ano**	Součástí řešení je sestavení více IPsec Site2Site VPN pro bezpečný přístup do provozního a testovacího prostředí s ukončením VPN dle požadavku zákazníka.
Změny a provoz na testovacím či vývojovém prostředí nesmí ovlivnit provozní prostředí.	**Ano**	Prostředí jsou logicky oddělená a změny a provoz na testovacím či vývojovém prostředí neovlivní provozní prostředí.
Nedílnou součástí realizace je průběžná správa VPN připojení včetně přidání a modifikace VPN tunelů a sledování bezpečnostních incidentů.	**Ano**	Součástí řešení je průběžná správa VPN připojení včetně přidání a modifikace VPN tunelů a sledování bezpečnostních incidentů.

Definice požadavku	Splněno Ano/Ne	Způsob splnění
Pro každé datové centrum ve všech bezpečnostních doménách služba NTP časového normálu.	**Ano**	V každém datovém centru je dostupný NTP server.
Pro každé datové centrum ve všech bezpečnostních doménách služba SMTP relay pro odesílání mailů (pro doménu LOCAL i přijímání mailů).	**Ano**	V každém datovém centru a všech bezpečnostních doménách je dostupný SMTP relay pro odesílání mailů (pro doménu LOCAL i přijímání mailů).
Pro každé datové centrum ve všech bezpečnostních doménách služba DNS.	**Ano**	V každém datovém centru a všech bezpečnostních doménách je dostupná služba DNS.
Pro každé datové centrum ve všech bezpečnostních doménách přístup na definované služby v internetu – pro doménu DMZ oddělení min. plně stavovým firewallem, pro doménu LOCAL úplným oddělením (proxy), případně firewallem s plnou inspekcí paketů na 7 vrstvě ISO OSI modelu. Nedílnou součástí je správa firewallů	**Ano**	V každém datovém centru je dostupný spravovaný, dedikovaný a plně stavový firewall FortiGate-VM00 v režimu Active-Passive s inspekcí na 7 vrstvě ISO OSI modelu a oddělení bezpečnostních domén. Každá bezpečnostní doména má v každém datovém centru dedikovanou vlastní VLAN.
Pronájem místa v primárním datovém centru, včetně napájení a konektivity: 1x rack 1U server, 140W, připojení do lokální bezpečnostní domény, 2x PSU. Zajištění fyzického přístupu k zařízením spolu s poskytovatelem.	**Ano**	Součástí nabídky je požadovaný pronájem místa v primárním datovém centru, včetně napájení a konektivity: 1x rack 1U server, 140W, připojení do lokální bezpečnostní domény. Zajištění fyzického přístupu k zařízením je zajištěno spolu s poskytovatelem.
Pronájem místa v primárním datovém centru, včetně napájení a konektivity: 2x rack 2U server, 140W, připojení do lokální bezpečnostní domény, 2x PSU. Zajištění fyzického přístupu k zařízením spolu s poskytovatelem.	**Ano**	Součástí nabídky je požadovaný pronájem místa v primárním datovém centru, včetně napájení a konektivity: 2x rack 2U server, 140W, připojení do lokální bezpečnostní domény. Zajištění fyzického přístupu k zařízením je zajištěno spolu s poskytovatelem.
Minimálně dalších 5U v datovém stojanu v primárním datovém centru.	**Ano**	Součástí nabídky je požadovaných 5U.

4 SEZNAM POŽADOVANÝCH VIRTUÁLNÍCH PROSTŘEDKŮ V DATOVÝCH CENTRECH

Název instance	Velikost RAM [GB]	Počet jader CPU	Velikost HDD [GB]	Rozhraní Ethernet 1Gb
Provozní aplikační server	24	4	200	1
Testovací aplikační server	8	2	20	1
Vývojový aplikační server	8	2	20	1
Provozní databázový server	8	2	855	1
Testovací databázový server	4	4	90	1
Vývojový databázový server	4	4	85	1
Provozní reverzní proxy server	3	2	20	1
Testovací reverzní proxy server	3	2	20	1
Vývojový reverzní proxy server	3	2	20	1
Poštovní server	0,5	1	154	1
Vývojový www server	8	2	50	1

Testovací www server	8	2	50	1
Provozní www server statických stránek	4	2	251	1
Provozní www server hlavních stránek	4	2	251	1
Eshop	4	2	251	1
Flowmon kolektor	4	4	508	4
AddNet workserver	4	2	40	3
Monet sonda	4	2	40	3

5 Požadovaná doba na zřízení služby

Zadavatel požaduje provést vytvoření cílového prostředí provozu Vitakarty, provést kompletní migraci virtuálních prostředí ze stávajícího prostředí a provést ověření funkčnosti provozního i záložního prostředí do 45 pracovních dnů od podepsání smlouvy.
Uchazeč se zavazuje předložit do 10 pracovních dnů od podepsání smlouvy vypracovat plán migrace, ze kterého bude jednoznačně vyplývat časový harmonogram, požadavky na součinnost zadavatele a bude rovněž obsahovat návrh předávacích testů pro ověření funkčnosti zřízené služby.

6 Požadovaná platební podmínky – dle smlouvy

Cena za zřízení služby bude fakturována po předání – ověření funkčnosti služby.
Cena za provozování služby bude fakturována kvartálně/měsíčně, vždy na počátku fakturovaného období.
Daňové doklady budou mít splatnost 30 dnů.

7 Výpovědní doba

Zadavatel garantuje využívání služby min. 2 roky od podpisu smlouvy, pokud nedojde k závažnému porušení smlouvy.
Následně platí výpovědní doba 3 měsíce.

8 SLA

8.1. Datové centrum bude garantovat SLA (Service Level Agreement), garantovanou dostupnost služby 99,95 % a vyšší, tj. maximální doba výpadku služby v průběhu roku nesmí přesáhnout 263 minut.

8.2. A současně platí, že doba každého jednoho souvislého výpadku nesmí být delší než 60 minut.

9 Samoobslužný uživatelský portál pro řízení a správu zdrojů

Zadavatel požaduje jako součást poskytovaných služeb „hostingu“ zpřístupnit uživatelský portál kde bude na základě přístupových oprávnění možno administrátorsky provádět níže uvedené operace

Definice základních vlastností portálu

Název položky	Popis položky	Požadované funkcionality
Orchestrace serverové virtualizace	Služba poskytující škálovatelný samoobslužný přístup k výpočetním zdrojům.	Vytvoření instance
		Pozastavení instance
	Správa a automatizace velké množiny počítačových zdrojů.	Smazání instance

	Schopná pracovat s běžně dostupnými technologiemi virtualizace.	Zastavení instance
	Podpora hypervisorů: VMware – plně kompatibilní se současnou provozovanou platformou.	Změna velikosti instance
	Možnost horizontálního škálování na standardním hardwaru bez proprietárních požadavků na hardware či software.	Vytvoření snapshotu
		Přiřazení veřejné adresy
	Garance CPU Ready Time do 100ms pro každou provozovanou instanci včetně reportování parametrů.	Oddělení veřejné adresy
	Přístup k výkonnostním grafům a SLA reportům instancí.	Přiřazení skupiny firewall pravidel
	Možnost instalace vlastního operačního systému instance z ISO obrazu.	Změna skupiny firewall pravidel
		Zobrazení výstupu konzole instance v prohlížeči
		Přidání/odebrání virtuálního síťového interface
		Spuštění instance
Orchestrace úložiště	Služba, která řídí vytváření, připojování a odpojování blokových zařízení k serverům.	Vytvoření volumu
	Umí spolupracovat s různými druhy uložišť, jako jsou např.: CEPH, CloudByte, Coraid, EMC (ScaleIO, Vmax VNX a XtremIO), GlusterFS, Hitachi Data Systems, IBM Storage (IBM DS8000, Storwize family, SAN Volume Controller, XIV Storage System a GPFS), Linux LIO, NetApp, Nexenta, Nimble Storage, Scality, SolidFire, HP (StoreVirtual a 3PAR StoreServ family) a Pure Storage.	Smazání volumu
	Je vhodný pro výkonově náročné aplikace, jako je databázové úložiště, rozšiřitelné souborové systémy a poskytuje přístup serveru na úroveň bloku úložiště.	Přiřazení volumu k instanci
	Poskytuje výkonné funkce pro zálohování dat uložených ve volumech blokové storage.	Oddělení volumu od instance

	Snapshoty mohou být obnoveny nebo použity k vytvoření nového volumu.	Rozšíření volumu
		Vytvoření volumu z volumu (klonování)
	Volume	
	- logická jednotka, úložný prostor s jedním souborovým systémem, typicky leží na jednom oddílu pevného disku, velikostí se může lišit od fyzického disku	Migrace volumu (asistovaná hostem)
	Přístup k výkonnostním grafům a reportům volumů.	QoS – limity v IOPS
	Snapshoty	Vytvoření snapshotu volumu
	- stav systému v určitém časovém okamžiku (na úložišti)	Smazání snapshotu volumu
		Vylistování snapshotů
		Vytvoření volumu ze snapshotu
Autentizace portálu	Identity služba zajišťující autentikaci skrze API klienta a autorizaci na vysoké úrovni.	Vytvoření role
		Smazání role
	Podporující 2-faktor autentizaci.	Vylistování rolí
		Vytvoření projektu/tenantu/vdc
		Smazání projektu/tenantu/vdc
	Role	Informace o projektu/tenantu/vdc
	-vytvoření a nastavení jednotlivých rolí podle jejich oprávnění	Vylistování projektů/tenantů/vdc
		Přiřazení uživatele do projektu/tenantu/vdc
	Tenant/Projekt	Odebrání uživatele z projektu/tenantu/vdc

	- skupina uživatelů používající omezené výpočetní zdroje	Vytvoření uživatelů
		Smazání uživatelů
		Vylistování uživatelů
		Nastavení hesla uživateli
		Přiřazení/odebrání rolí uživatelům
		Upravení informací o uživateli
Orchestrace sítí	Služba doručující NaaS (networking as a service) ve virtualním výpočetním prostředí.	Vytvoření sítě
		Smazání sítě
	Možnost vytvořit bohaté síťové topologie a konfigurovat pokročilé síťové politiky v cloudu v hybridním prostředí sdílené a dedikované platformy.	Seznam sítí
		Informace o síti
	Možnost nasazení plně dedikovaného síťového řešení pro zajištění min. plně stavového firewallu, případně firewallu s plnou inspekcí paketů na 7 vrstvě ISO OSI modelu.	Vylistování všech sítí
		Informace o jednotlivých sítí a mapování do VLAN/VXLAN
		Vytvoření Poolu IP Adres
		Smazání Poolu IP Adres
		Seznam Poolu IP Adres
		Informace o Poolu IP Adres
	Security Groups (SG)	Vytvoření routeru
	- slouží jako virtuální firewall, který řídí průtok dat pro jednu nebo více instancí. Ke každé SG je možné přiřadit pravidla, které umožňují průtok dat do nebo z instancí.	Smazání routeru
		Nastavení brány routeru
		Odebrání brány routeru

		Seznam routerů
	Veřejný Pool IP	Informace o routeru
	- služba, která nepoužívá DHCP, k instancím s přiřazenou Pool IP lze přistupovat z veřejné sítě.	Přidání sítě do routeru
		Odebrání sítě z routeru
		Vytvoření SG firewallu
		Smazání SG firewallu
		Vylistování SG firewallu
		Vytvoření pravidla v SG firewallu
		Smazání pravidla v SG firewallu
		Vylistování pravidel v SG firewallu
		Informace o pravidlech v SG firewallu
API	REST API slouží pro programový, uživatelský a administrátorský přístup k poskytnutým zdrojům ve sdílené cloudové platformě.	K API musí být dostupná kompletní dokumentace.
		API komunikace výhradně přes SSL.
		API příkazy musí být autentikovány a ověřeny.
CMDB (Configuration management database)	CMDB je zde jako centrální úložiště všech konfigurací systému, tak aby se dali ukládat ve verzovacím nástroji pro sledování a audit změn. CMDB slouží jako vstupní bod pro aktualizace, záplaty, opravy, updaty a upgrady systému.	Kontinuální konfigurace a řízení změn pro zachování konzistence napříč všemi komponentami.
		Centrální místo pro zjišťování současného stavu konfigurací komponent.
		Efektivní a automatizovatelné nasazení produkčních částí systému.

		Centrální místo pro zjišťování stavu systémů (IP, OS, verze instalovaných aplikací, atp.)
Logování, monitoring a události		Nástroj má schopnost exportovat svoje události do nadřazených systémů.
		Nástroj sbírá centrálně logy a zobrazuje je skrze webové rozhraní.