

KATALÓG SLUŽIEB

REZORTNÝ PRIVÁTNY CLOUD

Verzia dokumentu: 1.2 (092024)

OBSAH

1	Skratky a špecifické termíny.....	2
2	IaaS služby	3
2.1	Virtuálne servery.....	3
2.1.1	Podporované konfigurácie	3
2.1.2	Operačné prostredia	4
2.1.3	Virtuálne servery kategórie „S“	4
2.1.4	Virtuálne servery kategórie „M“	4
2.1.5	Virtuálne servery kategórie „L“	5
2.2	Systémové diskové priestory	5
2.3	Dátové disky	6
2.4	Sieťové služby	6
2.4.1	Ochrana perimetra.....	6
2.4.2	firewall a Sieťová segmentácia	7
2.4.3	Pripojenie do Internetu a Privátnych WAN sietí.....	7
2.5	systémové služby	7
2.5.1	Sieťové súborové systémy.....	7
2.5.2	Objektové dátové úložisko	8
2.5.3	Zálohovanie a obnova dát.....	8
2.6	orchestračná platforma Kubernetes	8
2.7	Virtuálny privátny cloud.....	8
3	Záver	10

1 SKRATKY A ŠPECIFICKÉ TERMÍNY

Zoznam a vysvetlenie všetkých skratiek alebo špecifických termínov používaných v dokumente.

P.č.	Skratka	Popis alebo vysvetlenie
1.	RPC	Rezortný privátny cloud
2.	DCC	Výpočtové centrum DataCentrum Cintorínska Bratislava
3.	DCK	Výpočtové centrum DataCentrum Kopčianska Bratislava
4.	ZVS	Záložné výpočtové centrum Tajov
5.	HA	High availability - Vysoká dostupnosť
6.	KVM	Kernel Virtual Machine
7.	VPC	Virtuálny privátny cloud

2 IAAS SLUŽBY

2.1 VIRTUÁLNE SERVERY

RPC poskytuje preddefinovanú sadu šablón/konfigurácií virtuálnych serverov pre okamžité použitie. Základnými konfiguračnými parametrami sú počet virtuálnych procesorových jadier a veľkosť dostupnej operačnej pamäte. Virtuálne stroje sú poskytované z viacerých klastrov fyzických strojov, ktoré sú hardvérovo identicky vybavené a konfigurované pre konkrétne použitie. Tento dizajnový princíp umožňuje izoláciu aplikačného softvérového vybavenia a jeho beh na výkonovo a ekonomicky najvýhodnejšom hardvérovom vybavení. Rozoznávame nasledovné klastre¹ podľa konfigurovanej virtualizačnej technológie²:

- Virtualizačná technológia VMware
 - Klastre tvorené systémami optimalizovanými pre beh databázových služieb Oracle
 - Klastre tvorené systémami optimalizovanými pre beh databázových služieb SAP HANA
 - Klastre tvorené systémami optimalizovanými pre beh aplikačných služieb Oracle
 - Klastre tvorené systémami optimalizovanými pre beh aplikačných služieb SAP S/4
 - Klastre tvorené systémami optimalizovanými pre beh open-source aplikačných a databázových služieb
- Virtualizačná technológia KVM
 - Klastre tvorené systémami optimalizovanými pre beh databázových služieb Oracle
 - Klastre tvorené systémami optimalizovanými pre beh aplikačných služieb Oracle
 - Klastre tvorené systémami optimalizovanými pre beh open-source aplikačných a databázových služieb

Zriaďovanie virtuálnych serverov v prostredí RPC zohľadňuje aj potreby na izoláciu a mieru overprovisioningu. Vďaka overprovisioningu je v prostredí RPC maximalizované využitie dostupných zdrojov. Existujú však aplikačné služby, pre ktoré použitie tejto funkcionality nie je prípustné a je teda deaktivovaná. Príkladom takýchto služieb sú napríklad inštancie SAP HANA.

2.1.1 PODPOROVANÉ KONFIGURÁCIE

Architektúra CPU všetkých virtuálnych serverov je x86-64. RPC disponuje fyzickými servermi s viacerými typmi procesorov. Všetky virtualizačné klastre sú však konfigurované so servermi vybavenými jedným druhom CPU. O umiestnení požadovaných virtuálnych serverov rozhoduje zriaďovateľ služieb tak, aby bola zabezpečená kompatibilita, certifikačné

¹ Klastre sú interným systémovým konfiguračným detailom RPC, ktorý zabezpečuje vysokú dostupnosť poskytovaných virtuálnych serverov. Voľba konkrétneho klastra je na zriaďovateľovi služieb na základe požiadaviek uvedených v onboarding manuáli.

² Virtualizačná technológia je interným systémovým konfiguračným detailom, ktorý zabezpečuje súlad cieľovej konfigurácie s licenčnými obmedzeniami konkrétneho softvérového vybavenia. Voľba konkrétnej virtualizačnej platformy je na zriaďovateľovi služieb na základe požiadaviek uvedených v onboarding manuáli.

požiadavky softvérového vybavenia a licenčné obmedzenia softvérového vybavenia prevádzkovaného na predmetných virtuálnych serveroch.

2.1.2 OPERAČNÉ PROSTREDIA

RPC štandardne poskytuje aktuálne a aplikačnými poskytovateľmi podporované nasledovné operačné prostredia:

- Red Hat Enterprise Linux 8 a 9
- Red Hat Enterprise Linux for SAP for Virtual Datacenters 8 a 9
- Red Hat Enterprise Linux for SAP Solutions for Virtual DC 8 a 9
- Rocky Linux 8 a 9
- Oracle Linux R8 a R9
- Ubuntu Linux 22.04 LTS a 24.04 LTS
- OpenSUSE Leap 15
- SUSE Linux Enterprise Server 15
- Debian 12
- Microsoft Windows Server 2019 a 2022

Základnými stavebnými komponentami RPC sú virtualizačné služby na báze VMware vSphere a KVM. V prípade potreby je možné vytvorenie obrazov ľubovoľného ďalšieho operačného prostredia podporovaného týmito technológiami.

2.1.3 VIRTUÁLNE SERVERY KATEGÓRIE „S“

Virtuálne servery kategórie „S“ sú vhodné ako aplikačné servery. Disponujú jedným až štyrmi virtuálnymi procesorovými jadrami a tomu zodpovedajúcou veľkosťou operačnej pamäte podľa nasledovnej tabuľky.

		Veľkosť operačnej pamäte v GB					
		2	4	8	12	16	24
Počet vCPU	1 (XXS)	XXS2	XXS4				
	2 (XS)		XS4	XS8	XS12	XS16	
	4 (S)			S8	S12	S16	S24

2.1.4 VIRTUÁLNE SERVERY KATEGÓRIE „M“

Virtuálne servery kategórie „M“ sú vhodné ako výkonné aplikačné, alebo databázové servery. Disponujú ôsmimi až šestnástimi virtuálnymi procesorovými jadrami a tomu zodpovedajúcou veľkosťou operačnej pamäte podľa nasledovnej tabuľky.

		Veľkosť operačnej pamäte v GB						
		16	24	32	48	64	128	256
Počet vCPU	8 (M)	M16	M24	M32	M48	M64		
	12 (XM)		XM24	XM32	XM48	XM64	XM128	
	16 (XXM)			XXM32	XXM48	XXM64	XXM128	XXM256

2.1.5 VIRTUÁLNE SERVERY KATEGÓRIE „L“

Virtuálne servery kategórie „L“ sú vhodné ako výkonné databázové servery, alebo servery na náročné výpočty a spracovanie dát. Disponujú dvadsiatimi až štyridsaťosem virtuálnymi procesorovými jadrami a tomu zodpovedajúcou veľkosťou operačnej pamäte podľa nasledovnej tabuľky.

		Veľkosť operačnej pamäte v GB							
		48	64	128	256	512	768	1024	1536
Počet vCPU	20 (L)	L48	L64	L128	L256	L512			
	24 (XL)		XL64	XL128	XL256	XL512	XL768		
	28 (XXL)			XXL128	XXL256	XXL512	XXL768	XXL1024	XXL1536
	32 (3XL)				3XL256	3XL512	3XL768	3XL1024	3XL1536
	48 (4XL)					4XL512	4XL768	4XL1024	4XL1536

2.2 SYSTÉMOVÉ DISKOVÉ PRIESTORY

S každým virtuálnym strojom je zviazaný jeden systémový disk. Používateľ má možnosť zvoliť si veľkosť systémového disku. Systémové disky sú určené výlučne pre inštaláciu samotných operačných prostredí, nie pre aplikačné dáta. Veľkosť systémového disku nie je zviazaná s konkrétnou šablónou, je teda si možné veľkosť zvoliť počas vytvárania virtuálneho stroja. Štandardné podporované veľkosti systémových diskov sú 10, 20, 40, 60, 80 a 120GB. V prípade neštandardnej potreby je možné zadefinovanie inej veľkosti systémového disku.

Všetky systémové disky sú vytvárané na diskových zariadeniach TIER1 vybavených SSD diskami s vysokou priepustnosťou. RPC však umožňuje definovať priepustnosť z pohľadu virtuálnych serverov tak, aby kritické systémy mali vždy garantovanú výkonnosť diskového subsystému. Nasledovná tabuľka definuje ponuku.

		Priepustnosť v IOPS		
		500	1000	2000
Kapacita v GB	10	L10	M10	H10
	20	L20	M20	H20
	40	L40	M40	H40
	60	L60	M60	H60

	80	L80	M80	H80
	120	L120	M120	H120

2.3 DÁTOVÉ DISKY

Aplikačné a databázové dátové diskové priestory sú sekundárnymi diskovými priestormi pridelenými virtuálnym strojom za účelom uchovávaní aplikačných dát. Virtuálny stroj môže byť vybavený ľubovoľným počtom takýchto dodatočných diskových priestorov.

Veľkosť diskových priestorov sa zhoduje s veľkosťami systémových diskových priestorov. Navyše sú však poskytované aj priestory s väčšími kapacitami, ako 240, 480, 960GB. Požadovaná kapacita, ako aj aplikačný dizajn rozhoduje o mixe diskových priestorov pridelených virtuálnym strojom.

Obdobne ako je tomu v prípade systémových diskov sú aj dátové disky zriaďované na diskových zariadeniach TIER1 vybavených SSD diskami s vysokou priepustnosťou. Taktiež sú k dispozícii s tromi úrovňami priepustnosti.

Kapacita dátových diskov je voliteľná v rozsahu do kapacity 5 TB podľa požiadaviek konkrétného systému. V prípade potreby väčšej kapacity sa zriaďuje väčší počet dátových diskov so sumárnou kapacitou zodpovedajúcou požiadavkám.

2.4 SIEŤOVÉ SLUŽBY

2.4.1 OCHRANA PERIMETRA

Medzi služby ochrany perimetra zaraďujeme služby zabezpečujúce bezpečný prístup k službám z externých prostredí a zároveň integráciu prostredí na služby poskytované v externých prostrediach. Služby s možnosťou zariadenia sú:

P. č.	Služba	Popis
1.	Perimetrový firewall	Ochrana pred hrozbami z externého prostredia.
2.	Load balancer	Služba rozkladania záťaže na viacero aplikačných serverov.
3.	SSL/TLS terminácia	SSL a TLS ukončovanie spojení na špecializovanom vysoko výkonnom zariadení F5.
4.	Terminálové služby	Terminálové služby pre prístup k službám prostredníctvom štandardizovaných virtualizovaných desktopových počítačov
5.	DMZ	Zriadenie sieťových segmentov DMZ pre potreby umiestnenia systémov s externým prístupom z Internetu.
6.	Dvojfaktorová autentifikácia	Bezpečná dvojfaktorová autentifikácia.

2.4.2 FIREWALL A SIEŤOVÁ SEGMENTÁCIA

RPC umožňuje v rámci prostredia tenantov nasadzovať viacero nezávislých prostredí. Popri produkčnom je bežné nasadenie jedného, alebo viacerých vývojových a testovacích prostredí. Tieto sú službami segmentačných firewallov sieťovo oddelené s exaktne riadenými prestupmi medzi nimi.

Definovanie prestupových pravidiel je súčasťou fázy zberu informácií o informačnom systéme v rámci onboarding procesu. Zakotvené sú v komunikačnej matici tenanta.

Služby v možnosťou zriadenia:

P. č.	Služba	Popis
1.	Segmentačný firewall – Izolácia tenanta	Izolácia tenanta na dedikované sieťové segmenty, VLAN a IP rozsahy.
2.	Segmentačný firewall – Vzájomné oddelenie prostredí	Interná sieťová segmentácia prostredia tenanta s oddelením jednotlivých prostredí.
3.	Segmentačný firewall – Segmentácia prostredí	Interná sieťová segmentácia jednotlivých prostredí a zriadenie oddelených portálových, aplikačných a databázových segmentov v rámci prostredí.

2.4.3 PRIPOJENIE DO INTERNETU A PRIVÁTNÝCH WAN SIEŤÍ

RPC umožňuje pripojenie zriaďovaného informačného systému do Internetu a privátnych sietí využitím nasledovných služieb.

P. č.	Služba	Popis
1.	Pripojenie do Internetu	Prístup do Internetu prostredníctvom proxy systému s nastavenými prístupovými pravidlami.
2.	Pripojenie do FINNET	Pripojenie do jednotlivých sietí FINNET.
3.	Pripojenie do GOVNET	Pripojenie do siete GOVNET.

2.5 SYSTÉMOVÉ SLUŽBY

2.5.1 SIEŤOVÉ SÚBOROVÉ SYSTÉMY

Sieťové súborové služby poskytujú vzdialené súborové úložisko pre ľubovoľné použitie. Dostupnosť úložiska je prostredníctvom protokolov NFS, FTP, alebo SFTP. Poskytované je dedikovaným virtuálnym serverom, ktorý je súčasťou architektúry tenanta RPC, ktorého služby ho konzumujú.

2.5.2 OBJEKTOVÉ DÁTOVÉ ÚLOŽISKO

Služby objektového úložiska sprístupňujú dátové úložiská prostredníctvom protokolu S3. Objektové úložiská predstavujú priestory pre dlhodobé uchovávanie dát a súborov pre potreby archivácie. Vhodné sú taktiež ako analytický a big data backend, alternatíva k sieťovým súborovým systémom a úložisko neštruktúrovaných dát a pre zálohovanie dát. Služby objektového úložiska sú poskytované dedikovaným virtuálnym serverom v prostredí tenanta, ktorého služby ho konzumujú.

2.5.3 ZÁLOHOVANIE A OBNOVA DÁT

Zálohovanie a obnova dát je v prostredí RPC riadená centrálné. Zastrešená je softvérovým vybavením Microfocus Data Protector a IBM TSM. Riešenie je dostupné pre celé prostredie RPC beh ohľadu na typ služieb, alebo operačné prostredia. Systém je kapacitne licencovaný a nepredstavuje žiadne obmedzenia na typ záloh.

Požiadavky na zálohovanie a obnovu sú predmetom onboarding manuálu. Na základe požiadaviek predmetného informačného systému je následne zabezpečené automatizované vykonávanie záloh ako aj pravidelné testy obnovy.

2.6 ORCHESTRAČNÁ PLATFORMA KUBERNETES

Podpora kontajnerizovaných aplikácií je zabezpečená orchestračnou platformou Kubernetes. RPC umožňuje zriadenie dedikovanej orchestračnej platformy v ľubovoľnom sieťovom segmente tenanta a tak prevádzku moderných mikroslužieb, alebo kontajnerizovaných aplikácií.

So službou zriadenia orchestračnej platformy sa viaže aj skupina podporných služieb, medzi ktoré patria:

P. č.	Služba	Popis
1.	Repozitár zdrojových kódov	Repozitár zdrojových kódov pre potreby realizácie CI/CD procesov.
2.	Repozitár obrazov aplikácií	Repozitár obrazov aplikácií.
3.	Bezpečnostná kontrola kvality kódu	Bezpečnostná kontrola kvality kódu a sledovanie zraniteľností.
4.	Systém pre deklaratívne nasadzovanie aplikácií	Systém pre deklaratívne nasadzovanie aplikácií.

2.7 VIRTUÁLNY PRIVÁTNY CLOUD

Virtuálny privátny cloud je privátna a izolovaná časť RPC pridelená konkrétnemu zákazníkovi. VPC má definovanú vlastnú sieťovú topológiu, ktorá je úplne nezávislá od sieťových topológií iných VPC a RPC ako takého. IP adresácia virtuálnych strojov je plne pod kontrolou zákazníka a nemusí byť zladžovaná s IP adresáciou RPC, alebo iných VPC. Je plne izolovaná.

Základnými komponentami VPC sú sieťové segmenty, virtuálne smerovače, verejné a privátne brány, používateľské VPN brány, VPN prepojenia do iných VPC a sieťové ACL.

3 ZÁVER

Služby RPC sú zriaďované na základe onboarding manuálu RPC. Všetky služby sú dostupné v oboch regiónoch, teda v regióne BA vo výpočtových centrách DCC a DCK, ako aj v regióne BB vo výpočtovom centre ZVS.

