SPCSS
Státní pokladna
Centrum sdílených služeb

Příloha č. 1

Technická specifikace Cloudových služeb

Obsah

SPCSS
Státní pokladna
Centrum sdílených služeb

1 Rozsah Cloudových služeb

1.1 Předpoklady vymezující Cloudové služby

V rámci přípravy Cloudových služeb byly vymezeny následující předpoklady a omezení pro 1. etapu, a to:

- Rozsah Cloudových služeb, který je uveden v této Nabídce může být doplňován na základě aktuálních potřeb plnění, na základě zjištění při poskytování činností v rámci Ostatních činností, avšak vždy formou navazující samostatné Výzvy na jejich rozšíření a postupem uvedeném v odst. V Smlouvy.
- Pro první iterace nebude použit backup ani v Azure ani v Azure Stack, rovněž v první iteraci nebude použit Sentinel, jen Firewall.
- Jediný přístup k resources v Azure bude v rámci sítě Poskytovatele přes VPN.

1.2 Přehled Cloudových služeb pro experimentální prostředí eSeL

Service category	Service type	Region	Description
Computer	Azure Kubernetes Service (AKS)	North Europe	Standard; Cluster management for 1 clusters; 3 D4a v4 (4 vCPUs, 16 GB RAM) x 730 Hours (Pay as you go), Linux; 2 managed OS disks – E6
Networking	IP Addresses	North Europe	Basic (Classic), 2 Dynamic IP Addresses X 730 Hours, 2 Static IP Addresses X 730 Hours
Networking	Virtual Network		North Europe (Virtual Network 1): 100 GB Outbound Data Transfer; North Europe (Virtual Network 2): 100 GB Outbound Data Transfer
Storage	Storage Accounts	North Europe	Block Blob Storage, General Purpose V2, Flat Namespace, LRS Redundancy, Hot Access Tier, 1,000 GB Capacity - Pay as you go, 10 x 10,000 Write operations, 10 x 10,000 List and Create Container Operations, 10 x 10,000 Read operations, 1 x 10,000 Other operations. 1,000 GB Data Retrieval, 1,000 GB Data Write, SFTP disabled
Storage	Azure Files	North Europe	SSD (Premium) Media tier, LRS Redundancy, Provisioned v1 Billing model, Provisioned capacity – 1,000 GiB Provisioned storage, 4,024 Provisioned IOPS, 203 MiB/sec Provisioned throughput, Pay As You Go, Used capacity - 0 GiB Used snapshot storage, 0 GiB Used soft-deleted storage

Service category	Service type	Region	Description
Networking	Application Gateway	North Europe	Application Gateway for Containers tier, 2 gateway quantity x 730 Hours, 1 frontends quantity x 730 Hours, 1 association quantity x 730 Hours, 1 capacity quantity x 730 Hours
Networking	VPN Gateway	North Europe	VPN Gateways, VpnGw1AZ tier, 730 gateway hour(s), 0 additional S2S tunnels (beyond included amount), 0 additional P2S connections (beyond included amount), 0 GB, Inter-VNET VPN gateway type
DevOps	Azure Monitor	North Europe	Log analytics: Log Data Ingestion: 1 GB Daily Auxiliary logs, 1 GB Daily Basic logs, 1 GB Daily Analytics logs ingested, 1 months of Interactive Retention, 0 months of Retention, 0 GB data restored for 0 days, 0 queries per day with 0 GB data scanned per query, 0 GB of Log Data Exported per day, Platform Log Data Processed per day: 1 GB with Destination to Storage or Event Hub and 0 GB with Destination to Marketplace Partners, 0 Search job Queries per day with 0 GB data scanned per query; 0 SCOM MI Endpoints; Managed Prometheus: Using estimated metrics volume estimation method (with a cluster of 1 AKS nodes, 10000 Prometheus metrics per node, and 30 metric collection intervals), 3 Average daily Dashboards users, 7 Dashboards, 50000 Data samples queried per dashboard, 25 promql alerting rules, 25 promql recording rules; Application Insights: 1 GB Daily logs ingested, 3 months Data retention, 0 Standard Web Tests, 5 Minutes Execution frequency, Executing for 730 hours; 0 resources monitored X 1 metric time-series monitored per resource, 5 Minutes Log Signal frequency with 0 Log Alerts monitored and 1 time series per signal, 0 Additional events, 0 Additional emails, 0 Additional push notifications, 0 Additional web hooks (in millions)
Compute	Azure Functions	North Europe	Consumption tier, Pay as you go, 128 MB memory, 1,000 milliseconds execution time, 3,600 executions/mo
Networking	Azure Firewall	North Europe	Standard tier, 1 Logical firewall units x 730 Hours, 10 GB Data processed

Service category	Service type	Region	Description
Containers	Azure Container Registry	North Europe	Standard Tier, 1 registry x 30 days, 10 GB Extra Storage, Container Build - 1 CPUs x 1 Seconds - Inter Region transfer type, 5 GB outbound data transfer from North Europe to West Europe

1.2.1 Technická specifikace Networking

VNet Název	Rozsah	Subnety	Poznámka
gw-vnet	/25		Pro App. GW a VPN
aks-vnet-1	/25 (128 IPs)	aks-subnet1 (/26 AKS nodes), service-subnet1 /26 služby)	
aks-vnet-2	/25 (128 IPs)	aks-subnet2 (/26 AKS nodes), service-subnet2 /26 služby)	
mgmt-vnet	/26		Monitoring etc.

1.2.2 Přehled uvažovaných resource group

Resource group	Služby v RG	Poznámka
RG-AKS	AKS cluster, AKS node pools, PVCs (File), VNet pro AKS	Vše spojené s AKS
RG-network	Application Gateway, VPN Gateway, public IP	Networking do SPCSS
RG-mgmt	Azure Monitor, Security Center, Azure Functions (log processing), CI/CD resources, AKS Container Registry	Monitoring a logování, vše pro nasazení a pipelines

1.2.3 Navrhované role pro Azure

Role	Popis	Permissions
Net-admin	Plný management sítě	Firewall, App GW, VPN GW, Routing, NSG
AKS-admin	Plný přístup k managementu AKS, storage a app. GW	Modifikace AKS, CNI apod., networking v rámci AKS RG, storage, monitoring
pipeline-user	Přístup pro nasazování a update ACR	deploy AKS, read storage, read/write ACR
AKS-developer	Přístup k AKS zdrojům – kubectl, nasazování, monitoring	AKS resources, Azure Monitor, claim storage

Role	Popis	Permissions
AKS-view	Read-only přístup	Read-only pro vše

1.2.4 Rozsah AzureStack

Přehled služeb pro 1. etapu

Resource	Instance	vCPU	vRAM	Disk OS	Disk APP	Sizing (počet)	RG	SRV
VM	Gitlab Runner	8	16	AZS_C1_8_16_WIN	AZS_MANAGED_DISK_128	1	0	1
VM	cdb-esel (eLeg)	8	16	AZS_C1_8_16_WIN	AZS_MANAGED_DISK_128, 4x AZS_MANAGED_DISK_1024 / PER VM	1	1	0
Služba	Gitlab (služba)	0	0	Služba SPCSS		Objem dat: 200 GB	0	1

1.3 Rozsah Cloudových služeb pro prostředí AI Assistant pro eSeL

Činnosti pro eSeL Assistant využívají pokročilé technologie zpracování přirozeného jazyka a jsou integrovány s cloudovou platformou Microsoft Azure, což zaručuje rychlé, přesné a bezpečné odpovědi na otázky uživatelů.
Rozsah Cloudových služeb pro prostředí eSeL AI Assistant (dále také „AI") je stanoven dle potřeb Objednatele.

2 Cena Cloudových služeb

Cena za přípravu Cloudových služeb je součástí Ostatních činností. Cena Cloudových služeb je členěná podle oblasti.

ID	Oblast Cloudových služeb	Odstavec	Cena za jeden kalendářní měsíc bez DPH	Cena za jeden kalendářní měsíc s DPH
1	Cloudové služby, z toho:	odst. 1	**268 859 Kč**	**325 319,39 Kč**
1.1	• Cloudové služby SPCSS pro experimentální prostředí – paušální měsíční platba;	odst. 1.2	87 657 Kč	106 064,97 Kč

ID	Oblast Cloudových služeb	Odstavec	Cena za jeden kalendářní měsíc bez DPH	Cena za jeden kalendářní měsíc s DPH
	• Cloudové služby Azure pro experimentální prostředí – měsíční platba dle skutečné spotřeby Azure		121 675 Kč	147 226,75 Kč
1.2	• Cloudové služby SPCSS pro AI – paušální měsíční platba; • Cloudové služby Azure pro AI – měsíční platba dle skutečné spotřeby Azure.	odst. 1.3	9 397 Kč 50 130 Kč	11 370,37 Kč 60 657,30 Kč

SPCSS
Státní pokladna
Centrum sdílených služeb

Podmínky využití poskytnutých informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách https://www.first.org/tlp/). Informace je označena příznakem, který stanoví podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Štítek	Podmínky použití
TLP: RED	Informace není určena pro jiné než určené osoby (určuje původce); poskytnutí informace dalším subjektům ze strany příjemce lze učinit pouze s předchozím souhlasem původce informace.
TLP: AMBER	Informaci je možné sdílet pouze s omezeným okruhem osob (určuje původce); příjemci mohou sdílet tyto informace pouze s členy své organizace a s dodavateli nebo zákazníky, kteří nezbytně potřebují tyto informace znát, aby se chránili nebo zabránili vzniku další škody; původce informace může rozsah sdílení dále omezit.
TLP: GREEN	Informace je určena k omezenému zveřejnění; omezeno na komunitu (organizace příjemce a další partnerské subjekty příjemce informace), avšak nikoliv s využitím veřejně dostupných komunikačních kanálů; příjemce nesmí informaci šířit mimo určenou komunitu (určuje původce).
TLP: CLEAR	Zveřejnění informace není omezeno; tímto ustanovením není dotčeno omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran.