

Státní pokladna Centrum sdílených služeb, s. p.

Na Vápence 915/14, Žižkov, 130 00 Praha 3

Počet listů: 22



MZV -LZ SMTP TEST (IaaS)

High level design

Datum: 8.4.2025



Obsah

1	Úvod	3
1.1	Klasifikace aktiva	3
1.2	Seznam použitých zkratk	3
1.3	Termíny realizace a zainteresované týmy	4
1.3.1	Zainteresované týmy za stranu SPCSS:	4
1.3.2	Zainteresované týmy za stranu zákazníka:	4
1.3.3	Provozní doba	5
1.3.4	Celková roční dostupnost	5
1.3.5		6
1.3.6	FQDN jméno pro aplikaci	6
2	Logický model řešení	6
2.1	Logický diagram	6
3	Technické řešení	7
3.1	Technický diagram	7
3.2	HW parametry	8
3.2.1	Virtualizační platforma	8
3.2.2	Storage	14
3.2.3	Databáze	15
3.2.4	FW throughput	15
3.2.5	VPN	16
3.2.6	HSM / KeyVault	16
3.2.7	Monitoring	16
3.2.8	Logování	17
3.2.9	Zálohování	18
4	Bezpečnostní požadavky	19
5	Podpisová doložka	21
	Informační proužek TLP pravidel	21
	Informační tabulka TLP pravidel	21

Tento dokument High-level design představuje šablonu s kapitolami, které jsou nutným minimem pro popis dodávaného řešení ve fázi vyjednávání se zákazníkem. Dokument obsahuje stručný úvod, 2 diagramy cílového stavu dle požadavků zákazníka, a to:

- diagram logického řešení*
- diagram technologického řešení,*

Dále termíny realizace a participující týmy jak za SPCSS, tak za zákazníka, a to ve formě názvů oddělení dle organizačních řádů SPCSS a zákazníka.

1 Úvod

Kapitola popíše hlavní náplň služby/řešení a jakým způsobem je služba/řešení poskytováno zákazníkovi a jaká jsou požadovaná SLA.

Zákazník MZV požaduje čerpat služby v úrovni IaaS pro shared služby. Jedná se o vytvoření společného prostředí pro služby. Služby slouží jako infrastrukturní pro obsluhu dalších aplikací například Drozd a CAFM.

1.1 Klasifikace aktiva

Kapitola popíše klasifikaci aktiva dle VoKB a požadavků zadavatele

IS KIS – informační systém kritické informační infrastruktury	VIS – významný informační systém	KS KII – komunikační systém kritické informační infrastruktury	IS ZS - informační systém základní služby	IS – informační systém nebo síť elektronických komunikací
☐	☐	☐	☐	☒

Kapitola popíše klasifikaci aktiva dle ZoISVS a vyhlášky o CC a požadavků zadavatele V případě, že se jedná o ISVS zaškrtnává se i klasifikace BÚ.

ISVS	BÚ 1	BÚ 2	BÚ 3	BÚ 4
☐	☐	☐	☐	☒

Ke klasifikaci aktiva uvádíme následující poznámku: Na základě provedeného hodnocení **dle aktuálně platné VoKB a ZoKB** byla provedena analýza rizik posilovaného IS s **výsledkem BÚ 3**. S ohledem na skutečnost, že program PROTOTYP má připravit dlouhodobě udržitelnou a bezpečnou platformu, byl rozhodnutím řídicího výboru schválen požadavek na zohlednění očekávané podoby transpozice NIS2 do návrhu architektury.

Výše uvedený požadavek předpokládá povýšení bezpečnosti předmětného systému na BÚ 4.

1.2 Seznam použitých zkratk

Uvedte seznam všech použitých zkratk v dokumentu. Jejich vysvětlení musí být pochopitelné pro všechny role zúčastněné na jednáních se zákazníkem.

Zkratka	Vysvětlení
---------	------------

1.3 Termíny realizace a zainteresované týmy

Kapitola popíše termíny realizace projektu v následující struktuře:

	Datum
Zahájení projektu :	Q2 2025
Zahájení implementace:	Q2 2025
Uvedení do provozu TEST:	Q4 2025 nejpozději do 31.10.2025
Ukončení implementace:	Q4 2025
Ukončení provozu řešení:	Není relevantní

1.3.1 Zainteresované týmy za stranu SPCSS:

[tým SPCSS, který zakázku připravuje zde vloží zainteresované role a oddělení za stranu SPCSS]

1.3.2 Zainteresované týmy za stranu zákazníka:

[tým zákazníka, který zakázku připravuje zde vloží zainteresované role a oddělení za stranu zákazníka]

1.3.2.1 SPOC Zákazník

1.3.2.2 SPOC Dodavatel

1.3.3 Provozní doba

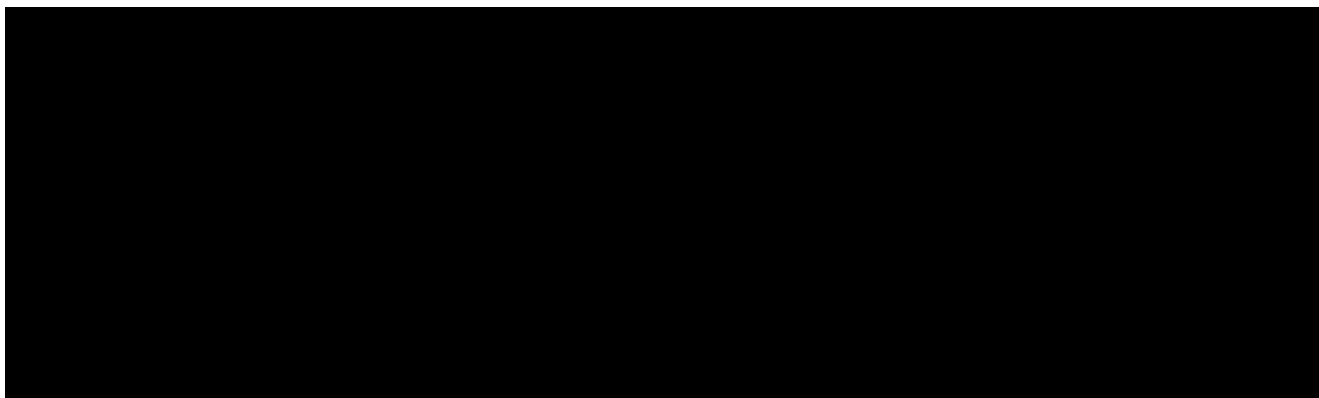
Kapitola popíše požadovanou provozní dobu zákazníkem

Provozní doba	
8x5 (TEST)	☒
24x5	☐
24x7	☐

1.3.4 Celková roční dostupnost

Kapitola popíše zákazníkem požadovanou celkovou roční dostupnost.

TEST	Typ SLA	Doba vyřešení kritické závady				ISVS
		4 hodiny	8 hodin	12 hodin	24 hodin	BÚ
☒	96,16 %	☐	☐	☐	☒	1
☐	99,45 %	☐	☐	☐	☐	2
☐	99,9 %	☐	☐	☐	☐	3
☐	99,982 %	☐	☐	☐	☐	3
☐	99,99 %	☐	☐	☐	☐	4



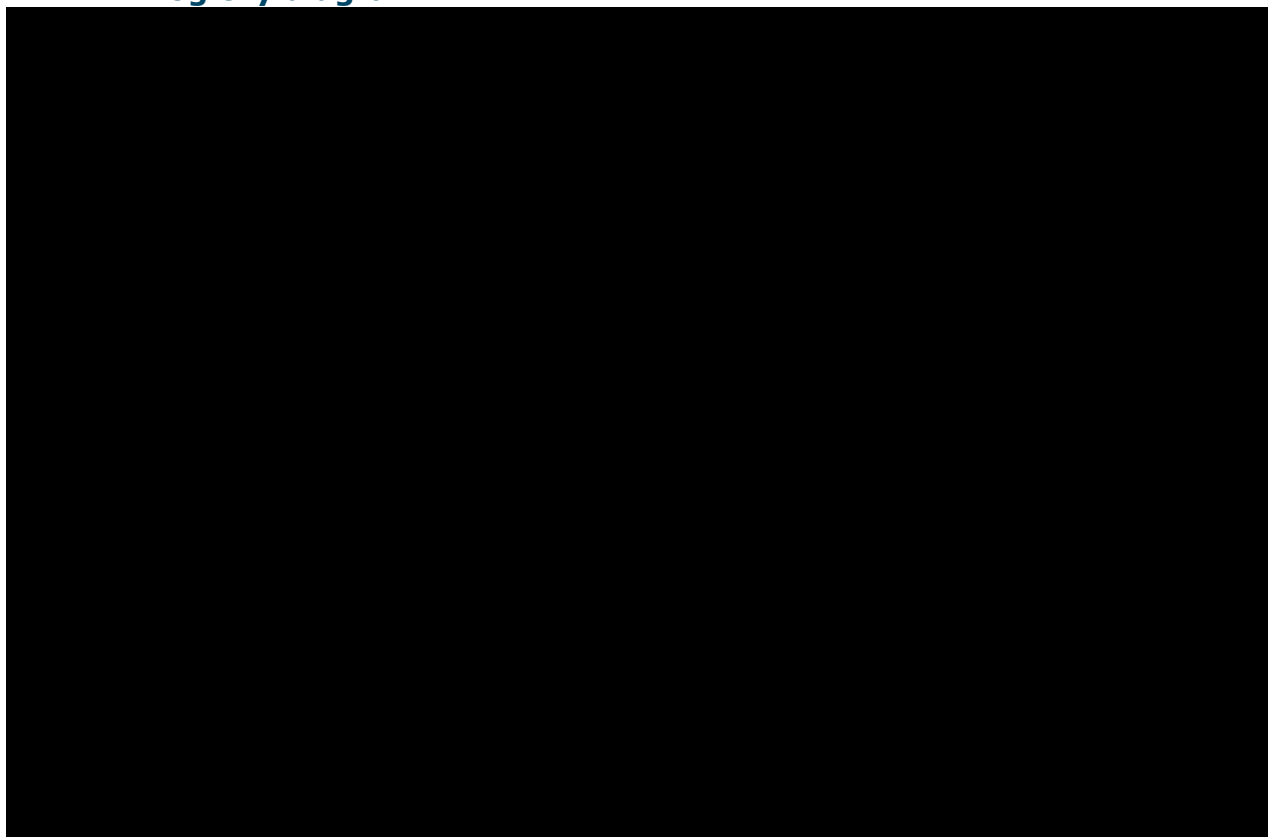
1.3.6 FQDN jméno pro aplikaci

Kapitola popíše zákazníkem požadované FQDN jméno pro provozovanou aplikaci

Jméno aplikace	FQDN jméno

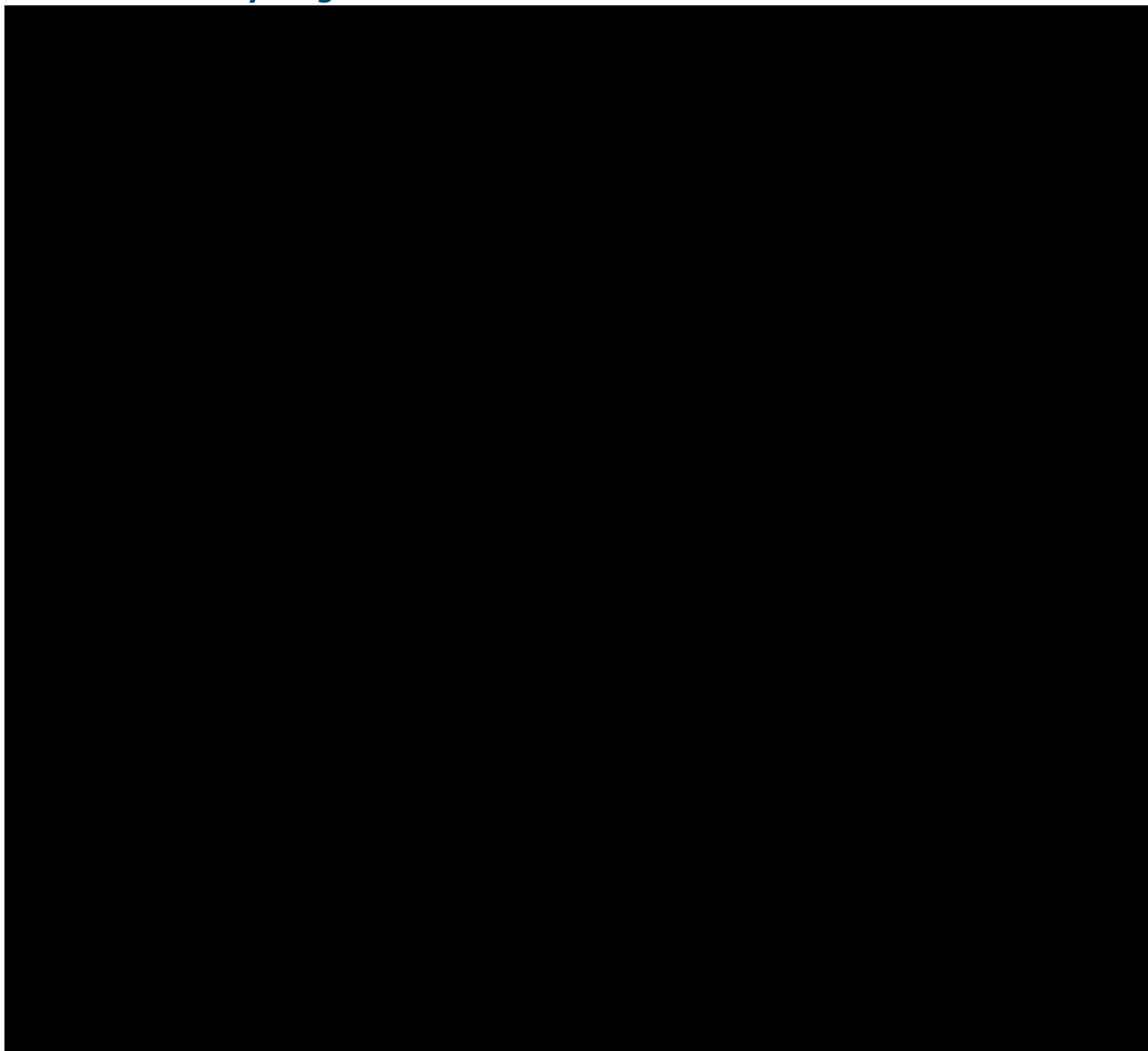
2 Logický model řešení

2.1 Logický diagram



3 Technické řešení

3.1 Technický diagram



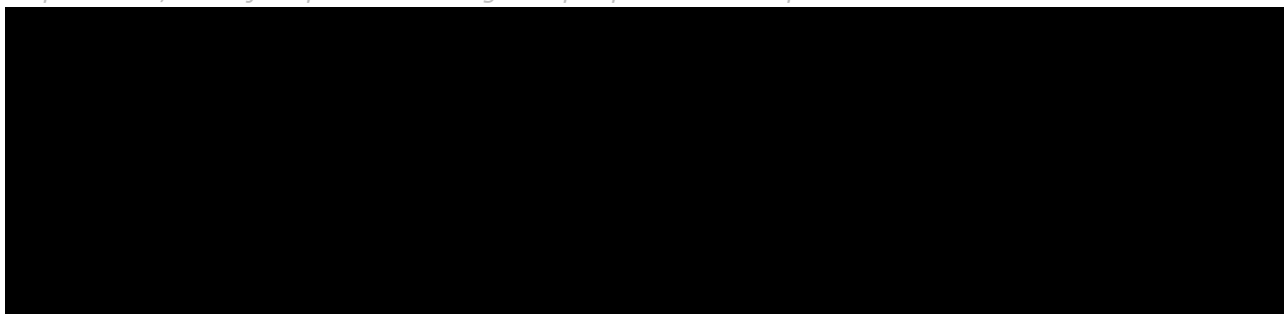
Pro ostatní prostředí (testovací, školící, preprodukční) je vždy doplněna informace buď v textu případně diagramem příslušného prostředí.

3.2 HW parametry

Kapitola popíše HW parametry jednotlivých prostředí v jednotlivých datových centrech.

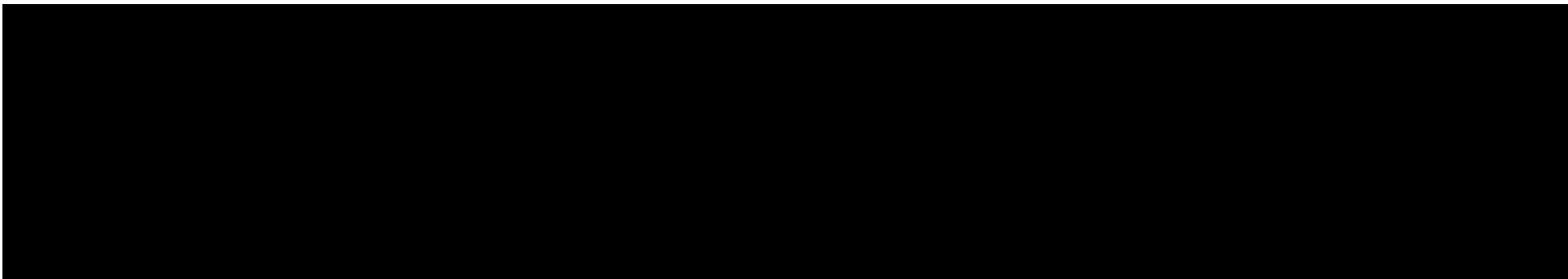
3.2.1 Virtualizační platforma

Kapitola popíše platformu, na které bude služba poskytována. Pokud se jedná o ISVS, lze vybrat jen platformu, která je zapsaná v katalogu CC pro příslušnou Bezpečnostní úroveň.



3.2.1.1 MS Azure

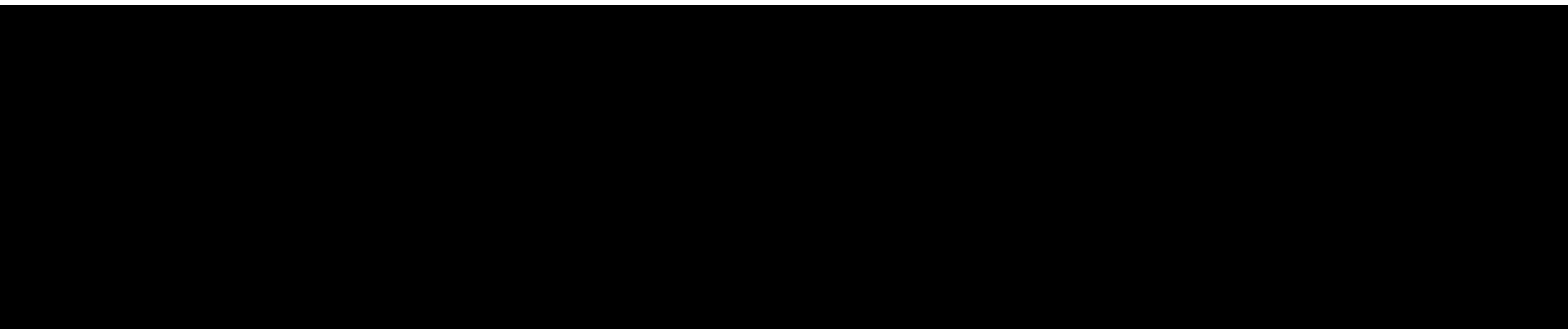
Kapitola popíše HW parametry prostředí Azure. V případě že nebude toto prostředí využito zapíše se není relevantní.

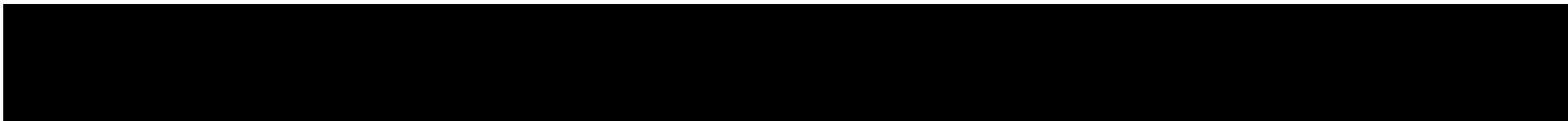


Bud' budeme zde doplňovat informace z Azure kalkulačky a dokument bude bobtnat anebo použijeme odkaz na přílohu, jako nedílnou součást a tam bude výjezd z azure kalkulačky.

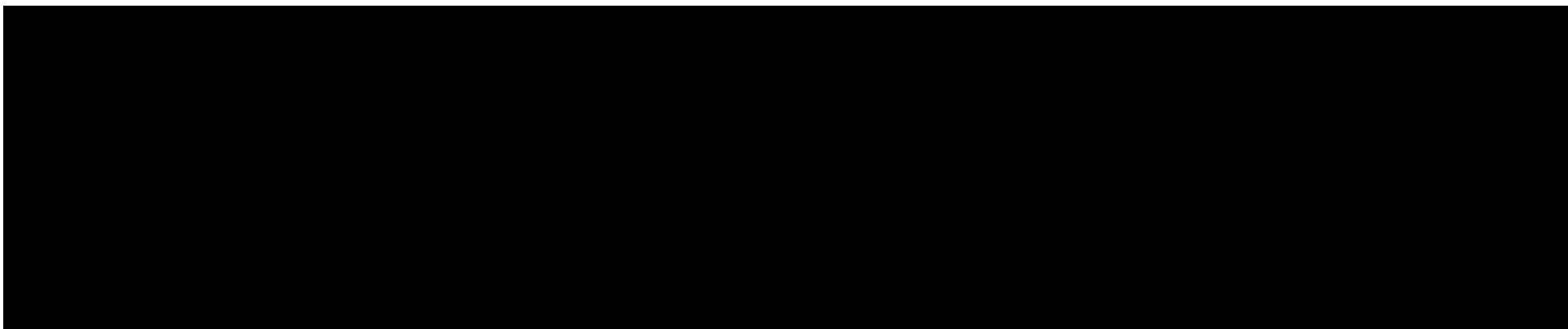
3.2.1.1.1 FinOps – MS Azure

Tato kapitola je zaměřena na FinOps a na představení strategií a nejlepších praktik pro efektivní správu nákladů a zdrojů v Microsoft Azure. Jak efektivně spravovat cloudové náklady, nejen aby byly udrženy v rozumných mezích, ale také aby byly v souladu s obchodními cíli a strategiemi. FinOps není jen o snižování nákladů; je to o vytváření hodnoty, transparentnosti a o optimalizaci investic, což umožňuje rychleji reagovat na tržní změny a inovovat.

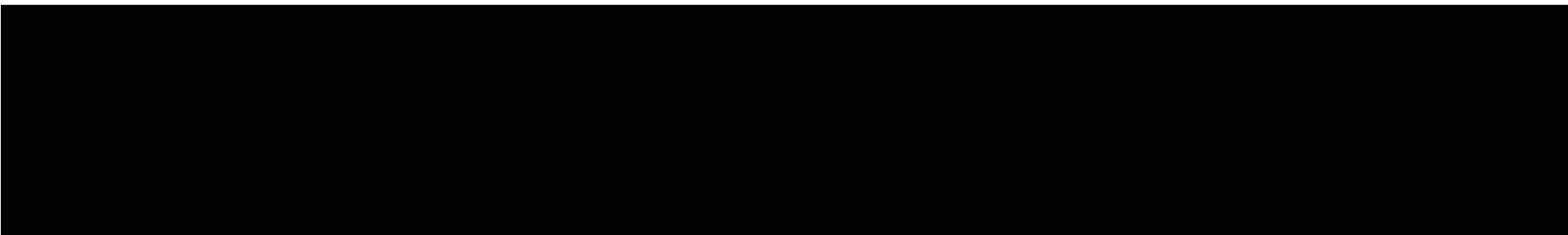




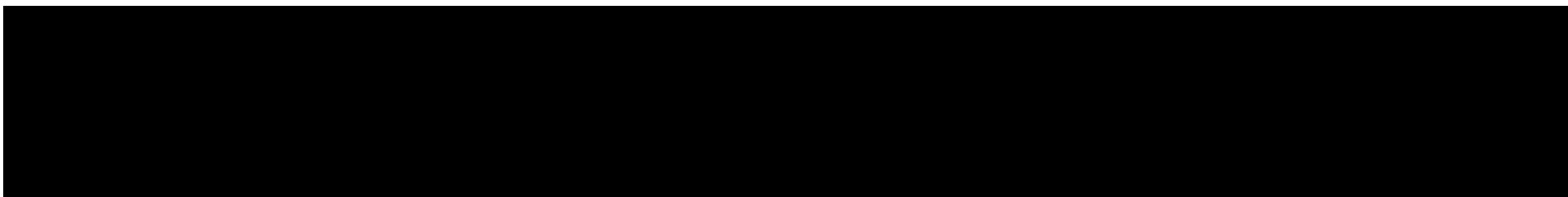
Politiky a governance, které v rámci FinOps jdou nastavit. Ideální nastavení je pro TEST a DEV, ale může být použito i pro produkční prostředí.



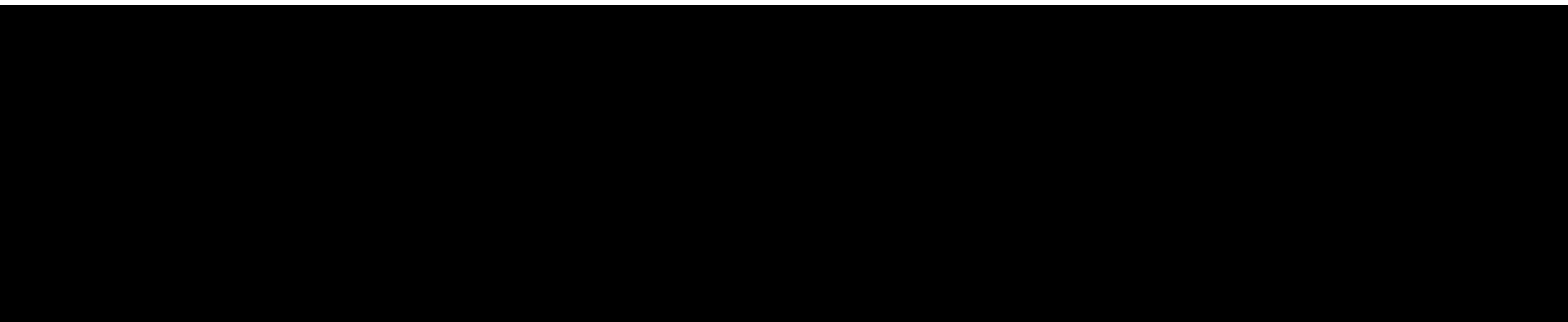
Budgety a rozpočty, které jdou nastavit na jednotlivá prostředí. A to jak se soft limitem, tak s hard limitem, kdy se po naplnění budgetu veškeré služby stopnou, než se obnoví limit další měsíc.



Automatické škálování znamená, že automaticky vytváříte nebo mažete zdroje dle utilizace a potřeby. Podmínky automatického škálování jsou dané dle pravidel, která si zvolí zákazník. Uplatňuje se u Virtual Machine Scale set (VMSS).



Azure Storage Account Lifecycle Management se týká správy životního cyklu dat ukládaných v Azure Storage. Azure Storage poskytuje široké možnosti pro ukládání dat, včetně objektů, disků, souborů a front, a zahrnuje nástroje a politiky pro efektivní správu těchto dat a jejich optimalizaci.

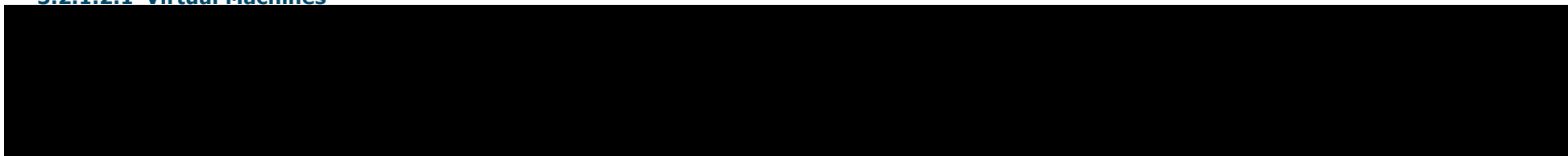


3.2.1.1.2 Poznámky

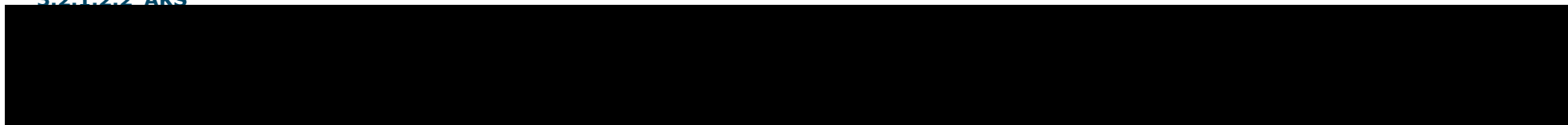
3.2.1.2 AzureStack Hub

Kapitola popíše HW parametry prostředí AzureStack. V případě že nebude toto prostředí využito zapíše se není relevantní.

3.2.1.2.1 Virtual Machines

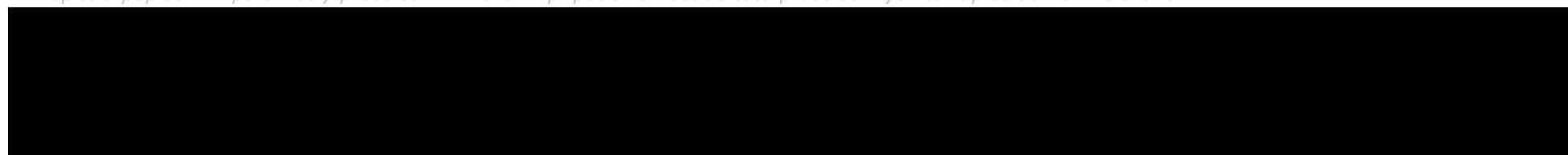


3.2.1.2.2 AKS



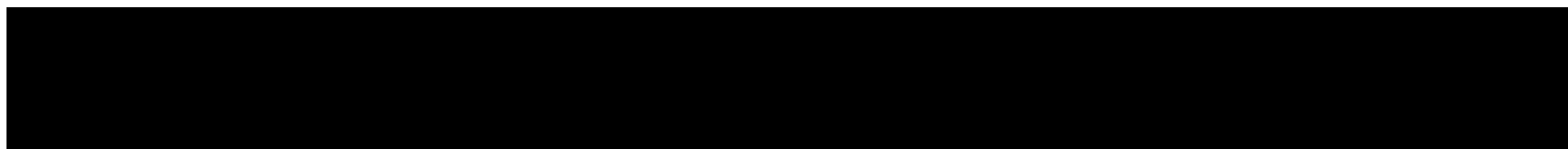
3.2.1.3 VMWare

Kapitola popíše HW parametry prostředí VMWare. V případě že nebude toto prostředí využito zapíše se není relevantní.



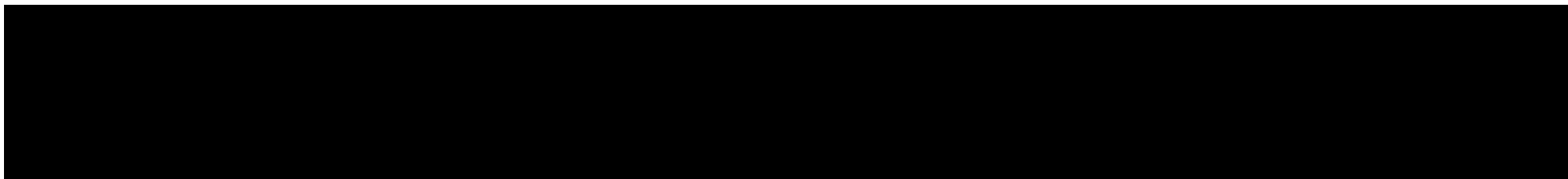
3.2.1.4 Power

Kapitola popíše HW parametry prostředí Power. V případě že nebude toto prostředí využito zapíše se není relevantní.



3.2.1.5 Google cloud

Kapitola popisuje HW parametry prostředí Google cloud. V případě že nebude toto prostředí využito zapíše se není relevantní.



3.2.2 Storage

Kapitola popíše velikost a umístění použitých diskových systémů nad rámec základní konfigurace virtuálních serverů, či Kubernetes clusterů.

[REDACTED]

3.2.2.1 MS Azure

[REDACTED]

3.2.2.2 MS AzureStack Hub

[REDACTED]

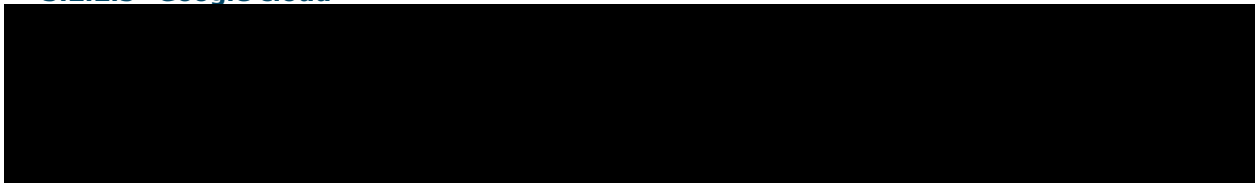
3.2.2.3 VM Ware

[REDACTED]

3.2.2.4 Power

[REDACTED]

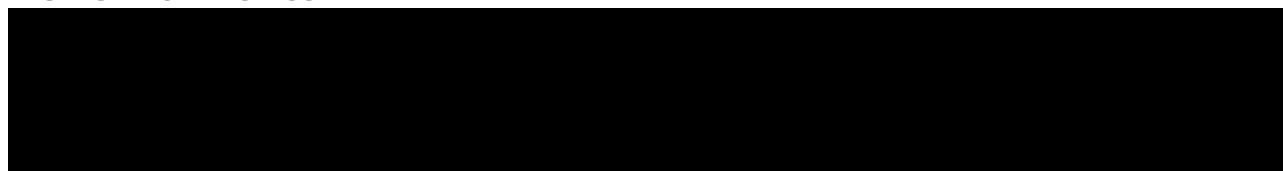
3.2.2.5 Google cloud



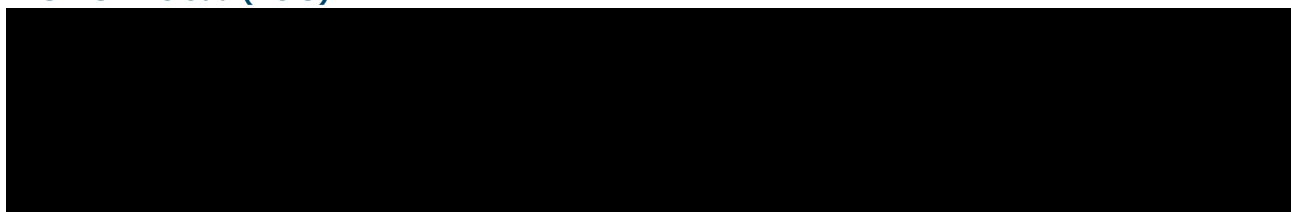
3.2.3 Databáze

Kapitola popíše požadavky zákazníka a jeho řešení na využití databází

3.2.3.1 On-Premise



3.2.3.2 Cloud (BÚ 3)



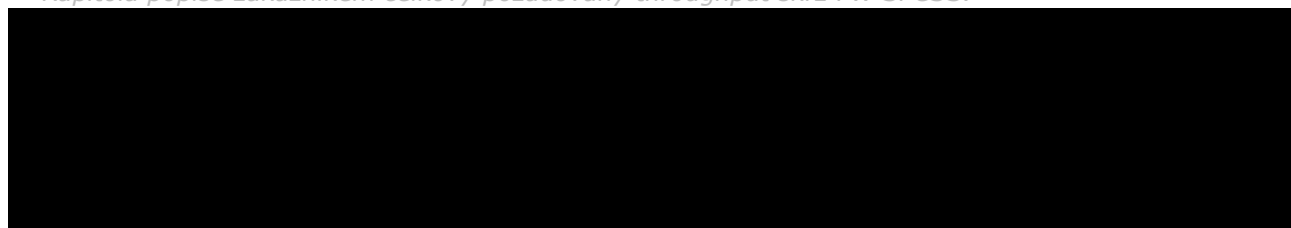
3.2.3.3 Poznámky

Kapitola popíše případné podrobnosti a požadavky na řešení DB.



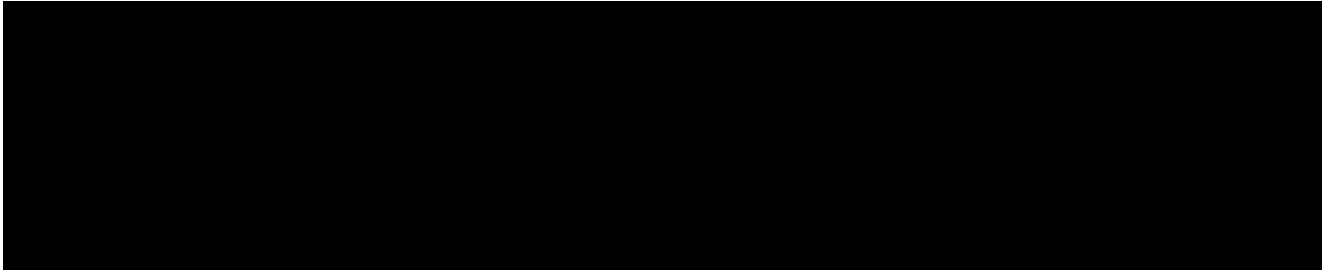
3.2.4 FW throughput

Kapitola popíše zákazníkem celkový požadovaný throughput skrz FW SPCSS.



3.2.5 VPN

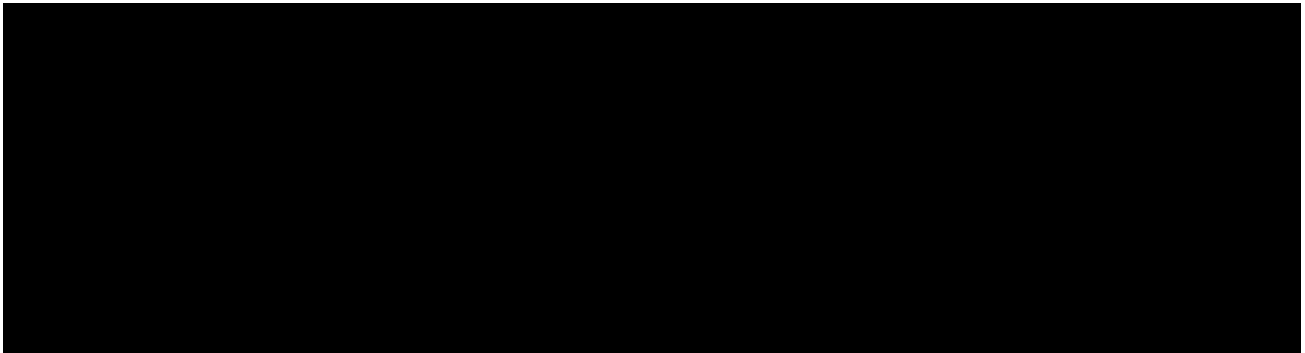
Kapitola popíše privátní VPN tunel, případně site-2-site tunely, které v rámci PoC vzniknou.



3.2.6 HSM / KeyVault

Kapitola popíše požadavky systému na použití HSM v on-premise, případně KeyVaultu v cloudu.

Dle V316/2021 - pro všechny BÚ musí poskytovatel šifrovat. Pro BÚ 2-4 UMOŽNÍ šifrování vybraným algoritmem dle NUKIB a u BÚ 3 - BYOK, u BÚ 4 - klíče v HSM (fips 104-2...)

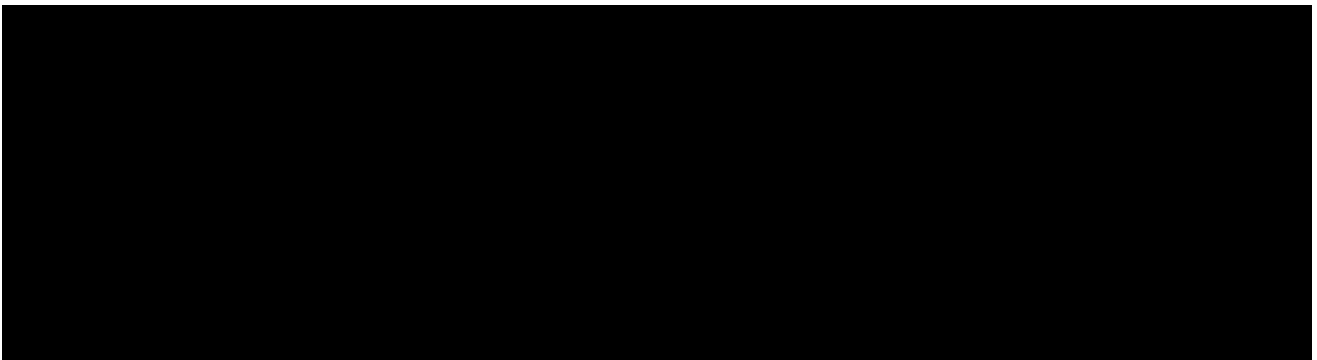


3.2.7 Monitoring

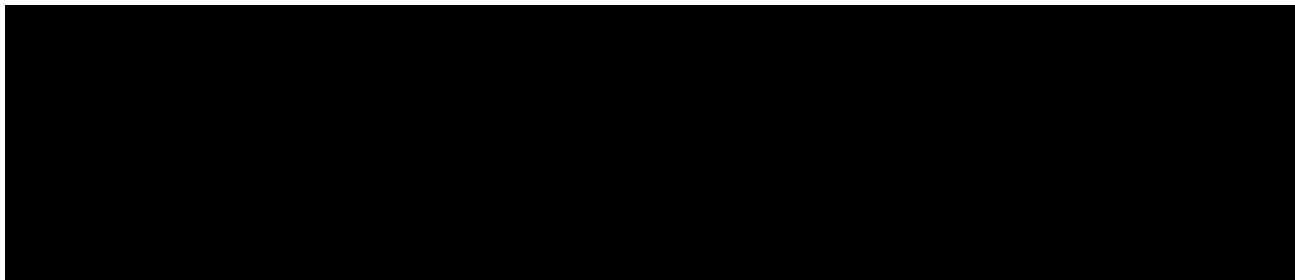
Kapitola popíše požadavky systému na jednotlivé typy monitoringu, které zákazník požaduje.

**V případě provozu ISVS nebo jeho části, musí být implementován Provozní monitoring, Bezpečnostní monitoring a Bezpečnostní monitoring databází pro BÚ (2-4). Platí pro On-premis i Cloud.*

3.2.7.1 On-premise



3.2.7.2 Cloud



3.2.7.3 Poznámky

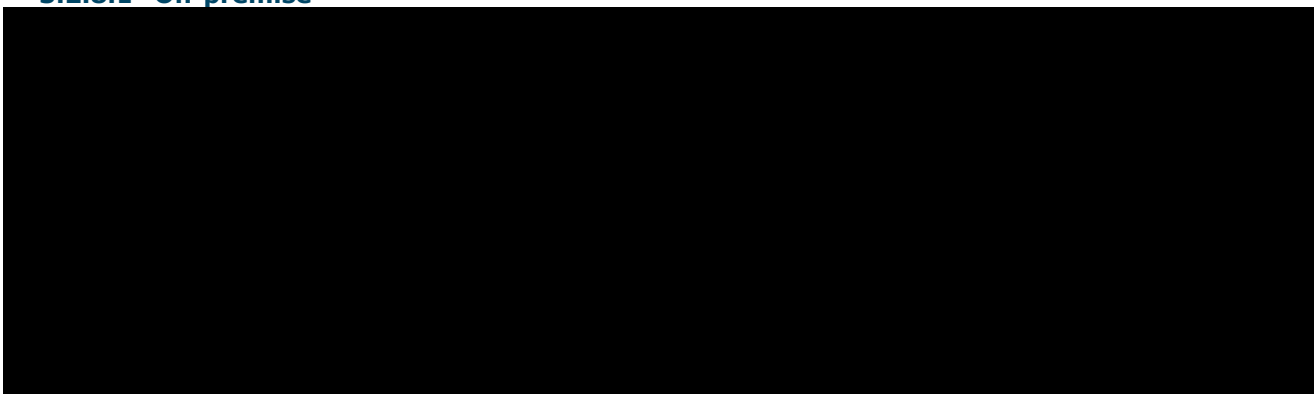
Kapitola popíše případné podrobnosti a požadavky na řešení jednotlivých typů monitoringu.

3.2.8 Logování

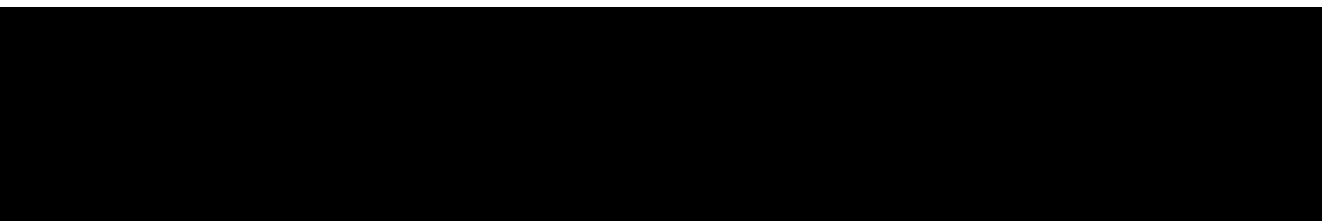
Kapitola popíše požadavky zákazníka na logování.



3.2.8.1 On-premise



3.2.8.2 Cloud



3.2.8.3 Poznámky

Kapitola popíše případné podrobnosti a požadavky na zasílání logů do SIEM/QRadaru.

VIS 12 měsíců (12 měsíců + 1 den), KII 18 měsíců (18 měsíců + 1 den).

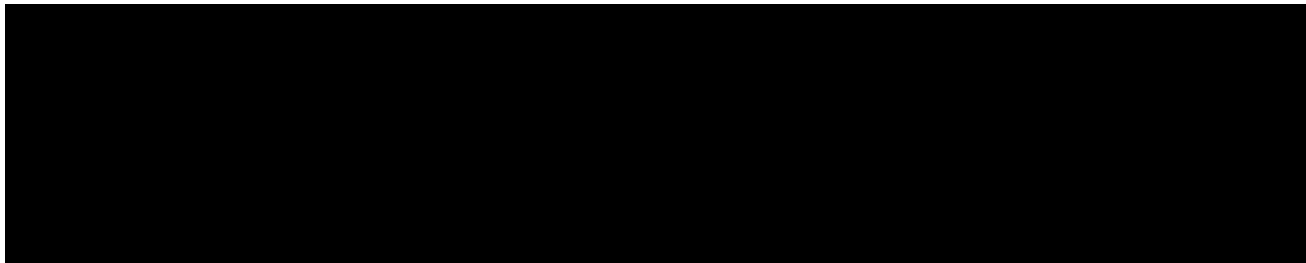


3.2.9 Zálohování

Kapitola popíše způsob, četnost a retenci záloh požadovaných systémem/dodavatelem aplikace

Četnost záloh – jak často bude záloha vykonávána

Retence záloh – jak dlouhou bude záloha uchována, než se smaže. Údaj je ve dnech



Poznámka:



5 Podpisová doložka

Informační proužek TLP pravidel

Příklad informačního proužku, který je vhodné umístit na konec dokumentu

Využití poskytnutých informací probíhá v souladu s metodikou **TLP** (Traffic Light Protocol) [Více informací zde>>](#)

Informační tabulka TLP pravidel

Příklad informační tabulky, kterou je vhodné umístit na konec dokumentu a vzhledem k její obsáhlosti i na novou stránku.

Podmínky využití poskytnutých informací	
Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách https://www.spcss.cz/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 ke sdílení , přístup je omezen na určené osoby (určuje původce/zdroj); poskytnutí informace dalším subjektům uvnitř i vně organizace příjemcem lze učinit pouze s předchozím souhlasem původce/zdroje informace.
TLP: AMBER+STRICT	Sdílení informace je omezeno na určené osoby (příjemce) a jejich organizace (určuje původce/zdroj) v souladu se zásadou „ potřebuje nezbytně znát “; příjemci nemohou dále sdílet tyto informace mimo svou organizaci bez předchozího souhlasu původce informace.

TLP: AMBER	Sdílení informace je omezeno na určené osoby (příjemce) a jejich organizace (určuje původce/zdroj); 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/zdroj 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.
Komunita: skupina, která sdílí společné cíle, zkušenosti a neformální důvěryhodnost. Komunita může být různě rozsáhlá – může například zahrnovat všechny odborníky na kybernetickou bezpečnost v zemi (nebo v sektoru či regionu). Organizace: skupina, která sdílí společnou příslušnost na základě formálního členství a je vázána společnými zásadami stanovenými organizací. Organizace může zahrnovat všechny členy organizace sdílející informace, ale jen zřídka je rozsáhlejší. Zákazníci: osoby nebo subjekty, které využívají služby organizace. Dodavatelé: osoby nebo subjekty, které organizaci dodávají služby či zboží.	