Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Odporúčanie

Príprava projektov ISVS pre ich zaradenie do „Cloud“ infraštruktúry

Február 2013

1. Úvod

Obsahom dokumentu je súhrn odporúčaní, ktoré bude potrebné akceptovať v procese prípravy projektov pre ISVS tak, aby tieto bolo možné v nasledovnom období začleniť do infraštruktúry „Cloud". Pri príprave dokumentu sa vychádzalo najmä z materiálov iných pracovných skupín pre Cloud v zahraničí, odporúčaní ENISA, pripravovaných štandardov NIST, z materiálov pracovnej skupiny pre Cloud pri NATO, ako aj z osvedčených postupov samotných výrobcov. Vydanie odporúčania bolo iniciované z podnetu pracovnej skupiny pri ITAS pre Government Cloud (ďalej len „WG GC").

Ide o prvý informatívny dokument obsahujúci odporúčania a kritériá pre „cloudovatelnosť infraštruktúry" určené pre novo pripravované projekty OPIS. Predpokladá sa, že nový prístup umožní v budúcnosti integrovať ISVS do Government Cloudu bez náročných dodatočných zmien a finančných nákladov.

Kritériá pre účely posudzovania projektov ISVS, predovšetkým projektov OPIS z pohľadu Cloud Computingu sú formulované v oblastiach taxonómie/terminológie, architektúry, bezpečnosti, z pohľadu modelu vyspelosti pre Cloud a IaaS služieb. Tento dokument má odporúčací charakter. Jeho ďalšie rozpracovanie do konkrétnych záväznejších foriem v súčasnosti riešia pracovné skupiny pod komisiou pre štandardizáciu informačných systémov verejnej správy na Ministerstve financií SR. V nasledovnom období pôjde predovšetkým o vydanie metodických pokynov, resp. aj zavedenie štandardizačných opatrení, ktoré si však vyžadujú dôslednú prípravu pre zaradenie do oficiálneho štandardizačného procesu.

Obsahom dokumentu sú kritériá s krátkym zdôvodnením, s odvolávkou na podrobnejší popis uvádzaný v prílohách.

Pre kladné posúdenie projektu je nevyhnutné aby boli splnené všetky nasledujúce časti.

Úroveň	Popis
Povinná funkcionalita	Musí byť daným posudzovaným projektom splnená
Odporúčaná funkcionalita	Všeobecné povinné zavedenie nie je z rôznych dôvodov vhodné, avšak zohľadňovanie danej funkcionality sa odporúča.

2. 1. Taxonómia

Detailná definícia vyžadovanej terminológie sa nachádza v Prílohe 1.

Kritérium	Názov	Úroveň	Spôsob hodnotenia	Príklad splnenia kritéria	Zdôvodnenie
1.1	Dodržať správnu Cloud terminológiu v rámci referenčnej taxonómie.	Povinná funkcionalita	Technická dokumentácia obsahuje rovnakú terminológiu	Uvedenie terminológie v zozname použitých skratiek.	Projekt nesmie definovať iný význam všeobecne využívanej terminológie pre oblasť Cloud computingu. Nakoľko existuje veľké množstvo hlavne anglických termínov, tak môžu vznikať rôzne interpretácie už pri prekladoch.

3. 2. Bezpečnosť

1.1. 2.1 Všeobecné podmienky pre hodnotenie vyspelosti v oblasti bezpečnosti projektu

Kritérium	Názov	Úroveň	Spôsob hodnotenia	Príklad splnenia kritéria	Zdôvodnenie
2.1.1	Dodržanie nasledujúcich všeobecných bezpečnostných podmienok: a) Vysoká dostupnosť (Podpora na úrovni komponentov konfigurácii architektúry) b) Konzistentná a predikovateľná konvergencia v prípade výpadku niektorého komponentu c) Možnosť virtualizácie infraštruktúry dátovej siete d) Možnosť izolácie dát jednotlivých konzumentov služieb e) Použitie mechanizmov na izoláciu VM f) Možnosť synchronizácie času g) Možnosť monitoringu komponentov h) Podpora dôvernosti a integrity prenášaných dát v rámci WAN i) Možnosť detekcie prienikov j) Možnosť logovania všetkých bezpečnostne relevantných udalosti k) Zálohovanie dát l) Možnosť nastavenia vlastných bezpečnostných politík konzumentom.	Povinná funkcionalita	Riešenie umožňuje zaistiť bezpečnosť informácií v oblasti dôvernosti, integrity a dostupnosti informácií.	Zavedenie organizačných a technických opatrení pre riešenie bezpečností informácií.	Všeobecné podmienky poskytujú Možnosť hodnotenia projektu z pohľadu prevádzky projektu a definujú základný rámec pre hodnotenie z hľadiska troch základných pilierov bezpečnosti a to dôvernosti, integrity a dostupnosti. Zvláštny dôraz je kladený na zabezpečenie dôvernosti dát.
2.1.2	Dodržanie nasledujúcich všeobecných bezpečnostných podmienok: a) Šifrovanie diskov VM a samotných VM b) Kontrola integrity VM c) Ochrana senzitívnych dát počas prenosu šifrovaním vrátane privátnych kľúčov hesiel atď. d) Možnosť zabezpečenia uložených dát prostredníctvom šifrovania e) Šifrovanie dát určených pre zálohovnie	Odporúčaná funkcionalita	Riešenie umožňuje nasadiť prostriedky šifrovania za účelom zabezpečenia ochrany dôvernosti, autentickosti a integrity informácií.	Ochrana dôvernosti, autentickosti a integrity informácií kryptografickými prostriedkami	Všeobecné podmienky poskytujú Možnosť hodnotenia projektu z pohľadu prevádzky projektu a definujú základný rámec pre hodnotenie z hľadiska troch základných pilierov bezpečnosti a to dôvernosti, integrity a dostupnosti. Zvláštny dôraz je kladený na zabezpečenie

					dôvernosti dát.

2.1. 2.2 Podmienky pre hodnotenie vyspelosti projektu v oblasti Autentizácia a Autorizácia

Kritérium	Názov	Úroveň	Spôsob hodnotenia	Príklad splnenia kritéria	Zdôvodnenie
2.2.1	Dodržanie bezpečnostných podmienok v oblasti autentizácie a autorizácie: a) Podpora adresárovej služby pre uloženie používateľských dát a pre overenie správcov/používateľov b) Podpora riadenia prístupových oprávnení na základe rolí c) Podpora password policy	Povinná funkcionalita	Riešenie umožňuje nasadiť prostriedky riadenia prístupu k informáciám podľa požiadaviek v oblasti riadenia prístupu.	Riadený autorizovaný prístup k informáciám.	Zabezpečenie správnej autentizácie a autorizácie je prvotným predpokladom pre zabezpečenie dôvernosti dát. Zavedenie multifaktorovej autentizácie zvyšuje dôveryhodnosť autentizácie.
	Dodržanie bezpečnostných podmienok v oblasti autentizácie a autorizácie: a) Podpora externého Identity providera b) Možnosť multifaktorovej autentizácie pre správu cloudu c) Možnosť multifktorovej autentizácie pre používateľov cloudu d) Podpora OAUTH	Odporúčaná funkcionalita	Riešenie umožňuje nasadiť prostriedky riadenia prístupu k informáciám podľa požiadaviek v oblasti riadenia prístupu.	Riadený autorizovaný prístup k informáciám.	Zabezpečenie správnej autentizácie a autorizácie je prvotným predpokladom pre zabezpečenie dôvernosti dát. Zavedenie multifaktorovej autentizácie zvyšuje dôveryhodnosť autentizácie.

3.1. 2.3 Kritéria pre hodnotenie vyspelosti prostredia určeného pre prevádzku projektu v oblasti bezpečnosti dátovej siete

Kritérium	Názov	Úroveň	Spôsob hodnotenia	Príklad splnenia kritéria	Zdôvodnenie
2.3.1	Dodržanie bezpečnostných podmienok v oblasti bezpečnosti dátovej siete: a) Podpora Multi-Tenant prostredia b) Podpora dôvernosti a integrity prenášaných dát v rámci LAN c) Možnosť vytvárania izolovaných zón, ktoré je možné manažovať samostatne d) Možnosť VLAN segmentácie e) Podpora virtuálnych firewallov, ktoré je možné manažovať z vlastného samostatného administratívneho rozhrania f) Možnosť Intrusion Detection/Možnosť	Povinná funkcionalita	Riešenie umožňuje dynamicky nasadzovať a konfigurovať ochranu informácií v dátových sieťach.	Použitá virtualizačná technológia prostriedkov dátových sieti a zároveň siete musia byť primerane riadené a spravované, čím sa zabezpečí ich ochrana pred hrozbami a udržanie primeranej bezpečnosti systémov a aplikácií využívajúcich sieťové prostredie, vrátane	Elementárnou podstatou projektu je poskytovať služby do externého prostredia prostredníctvom zabezpečených komunikačných kanálov. Podmienky pre bezpečnosť projektu z pohľadu prostredia, ktoré poskytuje služby prostredníctvom dátovej siete definujú rámec ako eliminovať

	Intrusion Prevention g) Možnosť Antivirovej/Antimalware kontroly h) Možnosť Data Leak Preventions i) Eliminácia útokov typu DoS, DDoS a SYN flood j) Eliminácia útokov na L7 k) Load balancing l) Web proxy m) Možnosť kompresie a cachingu HTTP n) Možnosť prevencie pred útokmi postavenej na geolocation			prenášaných informácií.	možné útoky na infraštruktúru projektu či už z externého alebo interného prostredia. Podpora Multi-Tenant prostredia infraštruktúry dátovej siete umožní prostredníctvom virtualizácie ponúknuť dedikované virtuálne prostredie (Možnosť ponúknutia doplnkových sieťových služieb na báze pridelenia dedikovaných prostriedkov vďaka virtualizácii sieťových komponentov).

4.1. 2.4 Kritéria pre hodnotenie vyspelosti prostredia určeného pre prevádzku projektu v oblasti súladu a auditu

Kritérium	Názov	Úroveň	Spôsob hodnotenia	Príklad splnenia kritéria	Zdôvodnenie
2.4.1	Dodržanie bezpečnostných podmienok v oblasti súladu a auditu: a) Splnenie podmienok, ktoré definuje Zákon č. 428/2002 Z. z. o ochrane osobných údajov, b) Splnenie podmienok, ktoré definuje Zákon č.275 o informačných systémoch verejnej správy, c) Splnenie certifikačných kritérií ISO/IEC 27001, d) Nezávislý audit vykonaný osobou, ktorá spĺňa kvalifikačné kritéria pre vykonanie auditu e) podľa stanovených regulačných a zákonných požiadaviek, f) Identifikácia aktív cloudu,	Povinná funkcionalita	Musia byť definovaný a zaistený súlad s legislatívnymi, bezpečnostnými politikami a normami organizácie. Naplánované a odsúhlasené požiadavky na audit a aktivity zahŕňajúce kontroly aby sa minimalizovalo riziko prerušení procesov organizácie.	Definované, dokumentované a udržiavané všetky významné zákonné, regulačné a zmluvné požiadavky a prístup organizácie na dosiahnutie týchto požiadaviek. Zavedené efektívne procesy auditu systému.	Cieľom hodnotenia podmienok súladu je stanoviť požiadavky a úroveň bezpečnosti s ohľadom na regulačné a zákonné požiadavky vzťahujúce sa na oblasť bezpečnosti prostredia, ktoré hostuje projekt. Cieľom riadenia aktív je dosiahnuť a udržiavať primeranú a efektívnu ochranu aktív organizácie. Klasifikácia aktív umožňuje stanoviť požiadavky na ich dôvernosť, integritu a

	g) Vypracovanie bezpečnostnej politiky.				dostupnosť a zároveň poskytuje podklady pre zabezpečenie primeraných opatrení na ochranu aktív. Pre dosiahnutie cieľa primeranej a efektívnej ochrany aktív je nevyhnutné spracovať zoznam aktív, ktoré budú umiestnené v prostredí. Zoznam aktív slúži ako podklad pre rizikovú analýzu a zároveň poskytuje informácie nevyhnutné na realizáciu plánov obnovy po havárii. Všetky aktíva musia byť identifikované v procese analýzy rizík. Pre jednotlivé aktíva by mali byť pri analýze rizík identifikované riziká. Všetky aktíva by mali byť pravidelne minimálne raz ročne inventarizované, čo napomáha zabezpečovaniu ich efektívnej ochrany.

5.1. 2.5 Kritéria pre hodnotenie vyspelosti prostredia určeného pre prevádzku projektu v oblasti manažmentu rizík

Kritérium	Názov	Úroveň	Spôsob hodnotenia	Príklad splnenia kritéria	Zdôvodnenie
2.5.1	Dodržanie bezpečnostných podmienok v oblasti manažmentu rizík: a) Identifikácia aktív b) Identifikácia hrozieb c) Identifikácia zraniteľností d) Identifikácia aké dopady na aktíva by	Povinná funkcionalita	Musia byť definované riziká spolu so stanovenými postupmi na základe ktorých budú stanovené postupy pre ich elimináciu, zníženie poprípade akceptáciu.	Identifikovaná metóda preskúmavania rizík ktorá vyhovuje identifikovanej bezpečnosti informácií organizácie, právnym a	Na stanovenie adekvátnych požiadaviek na bezpečnostné opatrenia za účelom eliminácie rizík a ich nežiaducich dôsledkov v prostredí, ktoré hostuje Cloud je podmienka

	mohli byť dôsledkom straty dôvernosti, integrity a dostupnosti. e) Analýza a ohodnotenie rizík f) Definovanie organizačno-technických opatrení na ošetrovanie rizík			regulačným požiadavkám. Identifikované, analyzované a ohodnotené riziká. Vybraté ciele riadenia a opatrenia na ošetrenie rizík.	vyhodnotiť úroveň hrozieb pre identifikované aktíva a rozsah zraniteľnosti aktív voči týmto hrozbám. Pri vypracovaní rizikovej analýzy odporúčame zohľadniť ISO/IEC 27005 a nevychádzať len zo súboru štandardných hrozieb, ale je nevyhnutné zohľadniť všetky faktory špecifických rizík, ktoré sú spojené s projektom ako hypervisor, izolálacia prostredia, manažment šifrovacích kľúčov, DMZ vrátane segmentácie dátovej siete atď. Pri analýze rizík si je nutné uvedomiť, že sa riziká spojené s prostredím, ktoré hostuje projekt sa neustále menia najmä ak sa mení technologické prostredie v ňom.

4. 3. Architektúra „Cloud ready“

Popis jednotlivých častí referenčnej architektúry sa nachádza v Prílohe 2.

Kritérium	Názov	Úroveň	Spôsob hodnotenia	Príklad splnenia kritéria	Zdôvodnenie
3.1	Adaptér prostriedkov a kontrola	Povinná funkcionalita	Navrhované technické riešenie umožní definovať celkovú architektúru bez nutnosti špecifikácie konkrétneho hardvéru.	Zavedenie virtualizačnej technológie na ktorej sa budú realizovať všetky infraštrukturálne požiadavky celkovej architektúry.	Nutná sada funkcií pre abstrakciu hardvéru a jeho manažment
3.2	Návrh šablón prostriedkov	Povinná funkcionalita	Navrhované technické riešenie musí umožniť definovanie štandardizovaných konfigurácií prostriedkov pre zabezpečenie infraštrukturálnych potrieb celkovej architektúry.	Zavedenie virtualizačnej technológie s možnosťou definovania šablón prostriedkov pre formovanie celkovej architektúry v kontexte definicií „IaaS služieb“ v kapitole 5.	Základná sada funkcií nevyhnutná pre štandardizáciu typov prostriedkov
3.3	Modelovanie kapacít prostriedkov	Odporúčaná funkcionalita	Riešenie poskytuje možnosti reportovania kapacít a dostupnosti prostriedkov a umožňuje mapovať požiadavky na prostriedky s dostupnými zdrojmi a ich koordináciu.	Použitá virtualizačná technológia má modul pre reportovanie kapacít prostriedkov ako aj užívateľské a aplikačné rozhranie pre ich manažment.	Sada funkcií pre manažment informácií potrebných pre autonómne riadenie prevádzky prostriedkov
3.4	Manažment životného cyklu prostriedkov	Odporúčaná funkcionalita	Riešenie umožňuje efektívny manažment fondu prostriedkov a jeho monitorovanie.	Použitá virtualizačná technológia disponuje užívateľským a aplikačným rozhraním pre manažment životného	Základné riadiace funkcie pre manažment prevádzky prostriedkov potrebné pre efektívne poskytovanie služieb

				cyklu prostriedkov a ich monitorovanie.	
3.5	Konfigurácia prostriedkov	Odporúčaná funkcionalita	Riešenie umožňuje dynamicky nasadzovať a konfigurovať kapacity prostriedkov.	Použitá virtualizačná technológia pomocou užívateľského a aplikačného rozhrania prijíma a realizuje konfigurácie kapacít prostriedkov.	Sada nevyhnutných funkcií pre automatizované nasadzovanie a konfiguráciu prostriedkov
3.6	Meranie využívania	Odporúčaná funkcionalita	Riešenie monitoruje dostupnosť a úroveň spotreby komponentov fondu prostriedkov a poskytuje takto získané informácie pre ďalšie procesovanie.	Použitá virtualizačná technológia má modul pre monitorovanie využívania prostriedkov a disponuje užívateľským a aplikačným rozhraním pre poskytovanie takto získaných informácií užívateľom a tretím stranám.	Funkcie zabezpečujúce informácie ohľadne využitia prostriedkov, nutné pre automatizovanú prevádzku služieb
3.7	Stav prostriedkov	Odporúčaná funkcionalita	Riešenie monitoruje chybové stavy komponentov fondu prostriedkov a poskytuje takto získané informácie informácie pre ďalšie procesovanie.	Použitá virtualizačná technológia má modul pre monitorovanie chybových stavov prostriedkov a disponuje užívateľským a aplikačným rozhraním pre poskytovanie takto získaných informácií užívateľom a tretím stranám	Funkcie zabezpečujúce informácie ohľadne dostupnosti prostriedkov, nutné pre automatizovanú prevádzku služieb
3.8	Katalóg prostriedkov a repozitár	Odporúčaná funkcionalita	Riešenie centralizuje a unifikuje manažment informácií ohľadne prostriedkov, ich kapacít	Použitá virtualizačná technológia pomocou užívateľského a aplikačného	Sada funkcií centrálneho manažmentu katalógu prostriedkov, ich konfigurácií a ich možných kompozícii,

			a konfigurácií.	rozhrania umožňuje manažment informácií ohľadne prostriedkov, ich kapacít a konfigurácií.	nevyhnutných pre poskytovanie štandardizovaných služieb

6.1. Zdôvodnenie

V súlade so stanovenými kandidátmi na IaaS služby je nutné aby projekty riadeným spôsobom (v súlade s Referenčnou architektúrou) pripravili svoje prostriedky pre ich budúce poskytovanie formou služby.

Vrstva "Dodávania zdrojov" a jednotlivé funkcie jej komponentov vo svojej podstate predstavujú rez cez funkcionality manažment systému generickej VM platformy. Logickým vyvodením tohto kritéria je povinnosť využitia virtualizácie všetkých prostriedkov v architektúre každého posudzovaného projektu, ako je zadefinované v kritériách IaaS služieb (5.1, 5.2, a 5.3).

5. 4. Model vyspelosti pre Cloud

Kritérium	Názov	Úroveň	Spôsob hodnotenia	Príklad splnenia kritéria	Zdôvodnenie
4.2	Architektúra a) Riešenie interoperability medzi homogénnymi celkami.	Povinná funkcionalita	a) Musí byť definovaný spôsob riešenia interoperability na báze aspoň jednej technológie (Kapitola Navrhovaný stav- Integrácia)	a) Zavedenie technológie pre riešenie interoperability (integračná technológia)	a) Dosiahnutie požadovanej úrovne interoperability, predstavuje predpoklad pre ďalšiu prepojiteľnosť v rámci Cloudu.
4.3	Infraštruktúra a) Štandardy infraštruktúry, ktoré budú použité v prevádzke b) Nasadzovanie určitých služieb automatickým/programatickým spôsobom	Povinná funkcionalita	a) Musia byť definované požiadavky na vypracovanie prevádzkových štandardov v rámci ktorých je/bude spracovaná aj infraštruktúra (Kapitoly: Navrhovaný stav- Prevádzka, Navrhovaný stav-Štandardy a legislatíva) b) Musia byť definované požiadavky/princípy ktoré umožnia automatické nasadzovanie aspoň niektorých služieb (Kapitoly: Navrhovaný stav- Integrácia, alebo Navrhovaný stav- Prevádzka)	a) Riešenie prevádzky a infraštruktúry na báze štandardov (napr. ITIL). b) Zavedenie metód a technológie pre automatické nasadzovanie služieb (napr. pomocou skriptov)	b) Programatické nasadzovanie, a jeho vyriešenie už počas projektu je predpokladom pre ďalšiu automatizáciu pri prevádzke v cloude. Je tiež východiskovou situáciou pri automatizovanom riešení škálovatelnosti.
4.4	Informácie a) Informačné aktíva sú popísane	Povinná funkcionalita	a) Musí byť definovaný princíp/požiadavka aby	a) Využitie jednotného popisu dát (napr.	a) Využitie spravovaných metadát, aj keď nie na

	pomocou metadát, avšak tieto metadáta nie sú spravované		informačné aktíva boli popísane formou metadát (dátových modelov) (Kapitola: Navrhovaný stav-dátová architektúra)	pomocu Schema Definition Language)	systematickej úrovni vytvára predpoklad pre jednotný popis informačných aktív. Táto vlastnosť je ďalej dôležitá pre vzájomnú prepojiteľnosť prevádzkovaných riešení v prostredí Cloudu.
4.5	Projekty, Portfólio a Služby a) Proces vývoj služieb b) Využitie SOA metodík minimálne počas projektu.	Povinná funkcionalita	a) Musí byť definovaný princíp/požiadavka na základe ktorého bude stanovený a dodržaný proces vývoja služieb (Kapitoly: Navrhovaný stav-Architektonické princípy, Plán implementácie) b) Spôsob prípravy a využitia SOA metodík musí byť stanovený v rozsahu limitovanom aspoň na úroveň vývojárskych tímov (Kapitoly: Navrhovaný stav-Architektonické princípy, Plán implementácie)	a,b) Využitie SOA governance	a) Zadefinovaný proces vývoja služieb vytvára nevyhnutný predpoklad pre harmonizáciu životného cyklu jednotlivých služieb, ktoré budú umiestnené v spoločnom Cloud prostredí. b) Úroveň aplikovania SOA metodík na jednotlivé služby priamo súvisí aj so zadefinovaným procesom vývoja. Jedná sa predovšetkým o kvalitatívne požiadavky, ktoré musia dosahovať úroveň keď SOA metodiky, ktoré budú v rámci projektu pripravené, musia byť zároveň aj použité.
4.6	Prevádzka, Správa a) Manažment dodržiavania SLA v rámci prevádzky služieb	Povinná funkcionalita	a) Musia byť definované kritéria/princípy na základe ktorých budú pre prevádzku jednotlivých služieb stanovené a vyhodnocované SLA (Kapitola: Navrhovaný stav-Prevádzka)	a) Stanovenie SLA pre jednotlivé služby	Riadenie a vyhodnocovanie SLA predstavuje jeden z podkladov pre neskoršie plánované poskytovanie voľných zdrojov.

4.7	Organizácia a) Vzdelávanie kľúčových pracovníkov	Povinná funkcionalita	a) Musí byť stanovený spôsob akým budú pracovníci s problematikou Cloud ready oboznamení/oboznamovaní (Kapitola: Navrhovaný stav-Organizácia)	a) Workshop, alebo tréning na tému Cloud ready.	a) Naplánované vzdelávanie kľúčových pracovníkov, ktorí sa budú podieľať na prevádzke a rozvoji riešenia je nevyhnutným predpokladom pre ďalšie úspešné zaradenie riešenia do Cloudu
4.8	Governance a) Využitie governance metodických prístupov	Povinná funkcionalita	a) Musia byť definované princípy/požiadavky na základe ktorých budú stanovené a dodržané EA a SOA governance prístupov uplatniteľných minimálne počas projektu. (Kapitoly: Navrhovaný stav-Architektonické princípy, Plán implementácie)	a) Zavedenie SOA a EA governance metodických prístupov pre realizáciu projektu	Požadovaná dosiahnutá úroveň SOA governance je v priamom súvise s požiadavkami kladenými na metodiky a procesy vývoja služieb.

6. 5. IaaS služby

Detailný popis navrhovaných typov IaaS služieb sa nachádza v Prílohe 3. Požiadavky na infraštruktúru musia byť definované tak aby umožnili vytvorenie Iaas Government Cloud Služieb podľa nasledujúcich kritérií.

Kritérium	Názov	Úroveň	Spôsob hodnotenia	Príklad splnenia kritéria	Zdôvodnenie
5.1	Podpora vytvárania služieb úložných zdrojov	Povinná funkcionalita	Navrhované technické riešenie má samostatne definované HW a SW prostriedky súvisiace	Definovanie parametrov (kapacita, rýchlosť, výkonnosť, dostupnosť) úložných	Požiadavky na "Službu úložných zdrojov" musia byť definované v povinných parametroch IaaS.Storage.1"

			s ukladaním údajov. Riešenie definuje spôsob merania využívania týchto zdrojov.	zdrojov (napr. diskových polí alebo spoločných úložných priestorov). Zavedenie monitoringu vyťaženia a obsadenia úložných zdrojov.	Požiadavky na "Službu úložných zdrojov" musia byť kategorizované podľa úrovní Iaas.Storage.2". Využívajú sa ponúkané služby riešenia "Služby úložných zdrojov" podľa úrovní Iaas.Storage.2 (min 1, max 3)
5.2	Podpora vytvárania služieb výpočtových zdrojov	Povinná funkcionalita	Navrhované technické riešenie má samostatne definované HW a SW prostriedky súvisiace s výpočtovými zdrojmi. Riešenie definuje spôsob merania využívania týchto zdrojov.	Definovanie parametrov (CPU, RAM, požadovaný úložný priestor) typizovaných výpočtových zdrojov. Zavedenie monitoringu prevádzky a vyťaženia výpočtových zdrojov.	Požiadavky na "Službu výpočtových zdrojov" musia byť kategorizované podľa úrovní "Iaas.Compute.1" Využívajú sa ponúkané služby riešenia "Službu výpočtových zdrojov" podľa úrovní Iaas.Compute.1 (min 1)
5.3	Podpora vytvárania služieb zálohovania	Povinná funkcionalita	Navrhované technické riešenie má samostatne definované HW a SW prostriedky súvisiace s riešením zálohovania. Riešenie definuje spôsob merania využívania týchto zdrojov	Definovanie parametrov úrovne dostupnosti (RPO, RTO vid. Príloha 3 Služby zálohovania). Zavedenie monitoringu využívania záloh a dodržiavania RPO a RTO.	Požiadavky na "Službu zálohovania" musia byť kategorizované podľa úrovní "Iaas.Backup.1". Požiadavky na "Službu zálohovania" musia byť definované v povinných parametroch "IaaS.Backup.2" Využívajú sa ponúkané služby riešenia "Službu zálohovania" zdroje podľa úrovní Iaas.Backup.1 (min 1, max 3)
5.4	Podpora pre Manažment Cloud služieb	Odporúčaná funkcionalita	Navrhované riešenie obsahuje samostatne definovanú funkcionalitu v odporúčanom rozsahu podľa Prílohy 3. Manažment Cloud služieb	Body 5.1, 5.2, 5.3 majú spoločnú funkcionalitu v oblasti definovania parametrov a monitoringu. Centralizácia tejto funkcionality ako aj jej rozšírenie do formy manažovaného	

				katalógu je splnením tohto kritéria.	

7.1. Zdôvodnenie

Štandardizácia jednotlivých typov IaaS služieb a ich parametrov vedie k redukcii komplexity manažmentu služieb a konfigurácií prostriedkov, čo v konečnom dôsledku zvýši efektivitu a ekonomické využitie infraštruktúry.

7. Príloha 1: Taxonómia/terminológia

Konzument Cloud služieb (Cloud Service Consumer)

Osoba alebo organizácia, ktorá udržiava obchodné vzťahy a zároveň využíva služby poskytovateľa Cloud služieb (Cloud Service Provider).

Poskytovateľ Cloud služieb (Cloud Service Provider)

Osoba, organizácia alebo entita zodpovedná za dostupnosť služieb konzumentom Cloud služieb (Cloud Service Consumer).

Cloud Carrier

Sprostredkovateľ, ktorý umožňuje prepojenie a prenos Cloud služieb medzi poskytovateľom Cloud služieb (Cloud Provider) a konzumentom (Cloud Consumer).

Sprostredkovateľ Cloud služieb (Cloud Broker)

Entita, ktorá spravuje využívanie, výkon a dodávku Cloud služieb. Zároveň má za úlohou udržiavanie vzťahu medzi poskytovateľom Cloud služieb (Cloud Provider) a konzumentom (Cloud Consumer).

Cloud Audítor (Cloud Auditor)

Entita, ktorej úlohou je vykonať nezávislý posudok Cloud služieb, informačných systémov, výkonnosti a zabezpečenia implementácie Cloud.

Cloud distribúcia (Cloud Distribution)

Proces transportu dát medzi poskytovateľmi Cloud služieb (Cloud Providers) a konzumentmi Cloud služieb (Cloud Consumers).

Prístup do Cloudu (Cloud Access)
Prístup do Cloud-u označuje proces nadviazania kontaktu so sprístupnením Cloud služieb.

Nasadenie služieb (Service Deployment)

Všetky aktivity, ktoré musí organizácia vykonať pre sprístupnenie Cloud služieb.

Orchestrácia služieb (Service Orchestration)

Označuje usporiadanie, koordinovanie a manažment Cloud infraštruktúry s cieľom poskytnutia rôznych Cloud služieb pre dosiahnutie IT a obchodných požiadaviek.

Manažment Cloud služieb (Cloud Service Management)

Manažment Cloud služieb zahŕňa všetky funkcie súvisiace so službami, ktoré sú nevyhnutné pre riadenie a prevádzku týchto služieb požadované zákazníkmi.

Súkromie (Privacy)

Súkromie alebo zabezpečenie údajov je správne, konzistentné zbieranie, spracovanie, sprostredkovanie, využívanie a nakladanie s osobnými údajmi (PI) a údajmi identifikujúcimi osoby (PII) počas ich celého životného cyklu.
(Zdroj: prevzaté z OASIS)

Softvér ako služba (SaaS)

Schopnosť poskytnutá koncovému spotrebiteľovi spočíva vo využívaní aplikácií poskytovateľa Cloud riešenia prevádzkovaných na Cloud infraštruktúre. Tieto aplikácie sú prístupné z rôznych klientskych zariadení prostredníctvom rozhrania tenkého klienta, akým je napríklad webový prehliadač (napr. webový e-mail). Spotrebiteľ neriadi a ani neovláda základné časti Cloud infraštruktúry, vrátane sietí, serverov, operačných systémov, úložiska údajov, alebo dokonca jednotlivých aplikačných schopností, snáď s výnimkou obmedzených užívateľsky špecifikovateľných konfiguračných nastavení aplikácie. (Zdroj: definícia NIST CC)

Platforma ako služba (PaaS)

Schopnosť poskytnutá koncovému spotrebiteľovi nasadiť na Cloud infraštruktúru spotrebiteľom vytvorené alebo získané aplikácie, vytvorené pomocou programovacích jazykov a nástrojov podporovaných poskytovateľom. Spotrebiteľ neriadi a ani neovláda základné časti Cloud infraštruktúry vrátane sietí, serverov, operačných systémov, úložiska údajov, ale má kontrolu nad nasadenými aplikáciami a prípadnými aplikačnými nastaveniami prostredia.
(Zdroj: definícia NIST CC)

Infraštruktúra ako služba (IaaS)

Schopnosť poskytnutá koncovému spotrebiteľovi spočíva v poskytnutí spracovania údajov, úložiska údajov, sietí a ďalších základných výpočtových zdrojov, ktoré je spotrebiteľ schopný nasadiť a využiť na beh ľubovoľného softvéru, ktorý môže zahrňovať operačné systémy a aplikácie. Spotrebiteľ neriadi a ani neovláda základné časti Cloud infraštruktúry, ale má kontrolu nad operačným systémom, úložiskom údajov, nasadenými aplikáciami, a prípadne obmedzenú možnosť nastavovať vybrané sieťové komponenty (napr. firewall). (Zdroj: definícia NIST CC)

Konzumovanie/využívanie služby (Service Consumption)

Cloud broker v roli aktívne využívajúci Cloud službu.

Poskytovanie služby (Service Provision)

Cloud broker v roli aktívne poskytujúci Cloud službu.

Bezpečnostný audit (Security Audit)

Systematické vyhodnotenie Cloud systému podľa toho, ako dobre zodpovedá súboru vopred stanovených bezpečnostných kritérií.

Audit dopadu na súkromie (Privacy-Impact Audit)

Systematické vyhodnotenie Cloud systému podľa toho, ako dobre zodpovedá súboru vopred stanovených kritérií s dopadom na súkromie.

Výkonnostný audit (Performance Audit)

Systematické vyhodnotenie Cloud systému podľa toho, ako dobre zodpovedá súboru vopred stanovených výkonnostných kritérií.

Sprostredkovanie služieb (Service Intermediation)

Sprostredkovateľ vystavuje službu, ktorá priamo zvyšuje hodnotu danej služby poskytnutej jednému alebo viacerým spotrebiteľom služby (service consumers), pričom pridaná hodnota rozširuje niektoré špecifické schopnosti služby. (Zdroj: Gartner)

Agregácia služieb (Service Aggregation)

Služba zabezpečujúca agregáciu zlučuje viac služieb do jedného alebo viacerých nových služieb. Tým je zabezpečené, že sú údaje modelované a integrované prierezom jednotlivých komponent služieb a zároveň sa tým zabezpečuje pohyb a bezpečnosť udajov prenášaných medzi konzumentom služby a viacerými poskytovateľmi služby. (Zdroj: Gartner)

Arbitráž služieb (Service Arbitrage)
Služba zabezpečujúca arbitráž, je obdoba agregácie Cloud služieb. Rozdiel medzi nimi je, že agregované služby nie sú stanovené. V skutočnosti je cieľom arbitráže poskytnúť flexibilitu a príležitostnú voľbu pre poskytovateľov služieb,
napr. agregátor, ktorý poskytuje viacero e-mailových služieb prostredníctvom jedného poskytovateľa služieb, alebo agregátor poskytujúci službu overovania solventnosti zákazníka medzi rôznymi agentúrami pri vyhodnocovaní poskytovania úverov. (Zdroj: Gartner)

Privátny Cloud (Private Cloud)

Infraštruktúra súkromného Cloud je prevádzkovaná výhradne pre potreby organizácie. Môže byť spravovaná organizáciou alebo treťou stranou, pričom fyzicky sa môže nachádzať na pôde organizácie alebo mimo. (Source: NIST CC Definition)

Komunitný Cloud (Community Cloud)

Infraštruktúru komunitného Cloud využíva niekoľko organizácií a podporuje konkrétne komunitu, ktorá zdieľa záujmy (napr. ciele, požiadavky na bezpečnosť, politiku a dodržiavanie záujmov). Infraštruktúru môžu spravovať organizácie alebo tretia strana, pričom fyzicky sa môže nachádzať na pôde organizácie alebo mimo. (Zdroj: definícia NIST CC)

Verejný Cloud (Public Cloud)

Infraštruktúra verejného Cloud je k dispozícii širokej verejnosti alebo veľkým komerčným skupinám, ale ostáva vo vlastníctve organizácie poskytujúcej služby Cloud. (Zdroj: definícia NIST CC)

Hybridný Cloud (Hybrid Cloud)

Infraštruktúra hybridného Cloud je kompozícia dvoch alebo viacerých typov Cloud (súkromný, komunitný alebo verejný), ktoré naďalej zostávajú jedinečnými entitami, ale sú spojené štandardizovanými alebo proprietárnymi technológiami, ktoré umožňujú prenositeľnosť údajov a aplikácií. (napr. Cloud bursting na vyrovnávanie záťaže medzi Cloud).

(Zdroj: definícia NIST CC)

Servisná vrstva (Service Layer)

Definuje základné služby vystavené poskytovateľmi Cloud služieb (Cloud Providers).

Fyzická vrstva prostriedkov (Physical Resource Layer)

Zahŕňa všetky dostupné fyzické prostriedky potrebné pre poskytovanie Cloud služieb.

Abstrakcia prostriedkov a riadiaca vrstva (Resource Abstraction and Control Layer)

Zahŕňa softvérové prvky, ako je hypervisor, virtuálne stroje, virtuálne úložisko dát a podporné softvérové komponenty, používané na realizáciu infraštruktúry, na ktorých sú postavené Cloud služby.

Prenositelnosť (Portability)

Schopnosť prenášať údaje z jedného systému do druhého, bez potreby znovu vytvárania alebo opätovného zadávania popisu údajov, prípadne významnej zmeny prenášanej aplikácie.
Schopnosť prevádzkovania softvéru alebo systému na viac ako jednom type alebo výkonnosti počítača, na viac ako jednom type operačného systému (viz. POSIX) pri zachovaní rovnakej prevádzkovej kvality.
[Zdroj: Federal Standard 1037C]

Interoperabilita (Interoperability)

Schopnosť komunikovať, spúšťať programy, alebo prenášať údaje medzi rôznymi funkčnými celkami, pri dodržaní vopred stanovených podmienok.
[Zdroj: American National Standard Dictionary of Information Technology (ANSDIT)]

Poskytovnie služieb/Konfigurácia (Provisioning/Configuration)

Proces prípravy a konfigurácie prostredia Cloud s cieľom zabezpečenia (nových) služieb svojim užívateľom.

Mobilné koncové body (Mobile Endpoints)

Fyzické zariadenie obvykle prenášateľné užívateľom, ktoré poskytuje Cloud službám a aplikáciám rozhranie človek / stroj. Mobilné koncové body môžu používať viacero metód a protokolov na pripojenie ku Cloud službám a aplikáciám.

Pevné koncové body (Fixed Endpoints)

Fyzické zariadenie na konkrétnom mieste, ktoré poskytuje Cloud službám a aplikáciám rozhranie človek / stroj. Pevný koncový bod obvykle používa jednu metódu a jeden protokol na pripojenie ku Cloud službám a aplikáciám.

Prenositeľnosť údajov (Data Portability)

Schopnosť prenášať údaje z jedného systému do druhého, bez potreby znovu vytvárania alebo opätovného zadávania údajov, prípadne významnej zmeny prenášanej aplikácie.
[Zdroj: Federal Standard 1037C]

Interoperabilita služieb (Service Interoperability)

Schopnosť komunikovať, spúšťať programy, alebo prenášať údaje medzi rôznymi Cloud službami, pri dodržaní vopred stanovených podmienok.
[Zdroj: upravené z American National Standard Dictionary of Information Technology (ANSDIT)]

Prenositeľnosť systémov (System Portability)

Schopnosť službu prevádzkovať na viac ako jednom type alebo veľkosti Cloud.
[Zdroj: upravené z Federal Standard 1037C]

Rýchle poskytovanie služieb (Rapid provisioning)

Automatická inštalácia Cloud systémov vykonaná na základe požiadaviek kladených na služby / zdroje / schopnosti.

Zmena prostriedkov (Resource change)

Konfiguračné nastavenia prostriedkov, zadávanie úloh na údržbu, modernizácie a pripojenie nových uzlov do Cloud.

Monitorovanie a reportovanie (Monitoring and Reporting)

Úlohou je sledovanie virtuálnych prostriedkov, monitorovanie vzniknutých udalostí počas prevádzky Cloud a vytváranie prehľadných správ o výkonnosti Cloud.

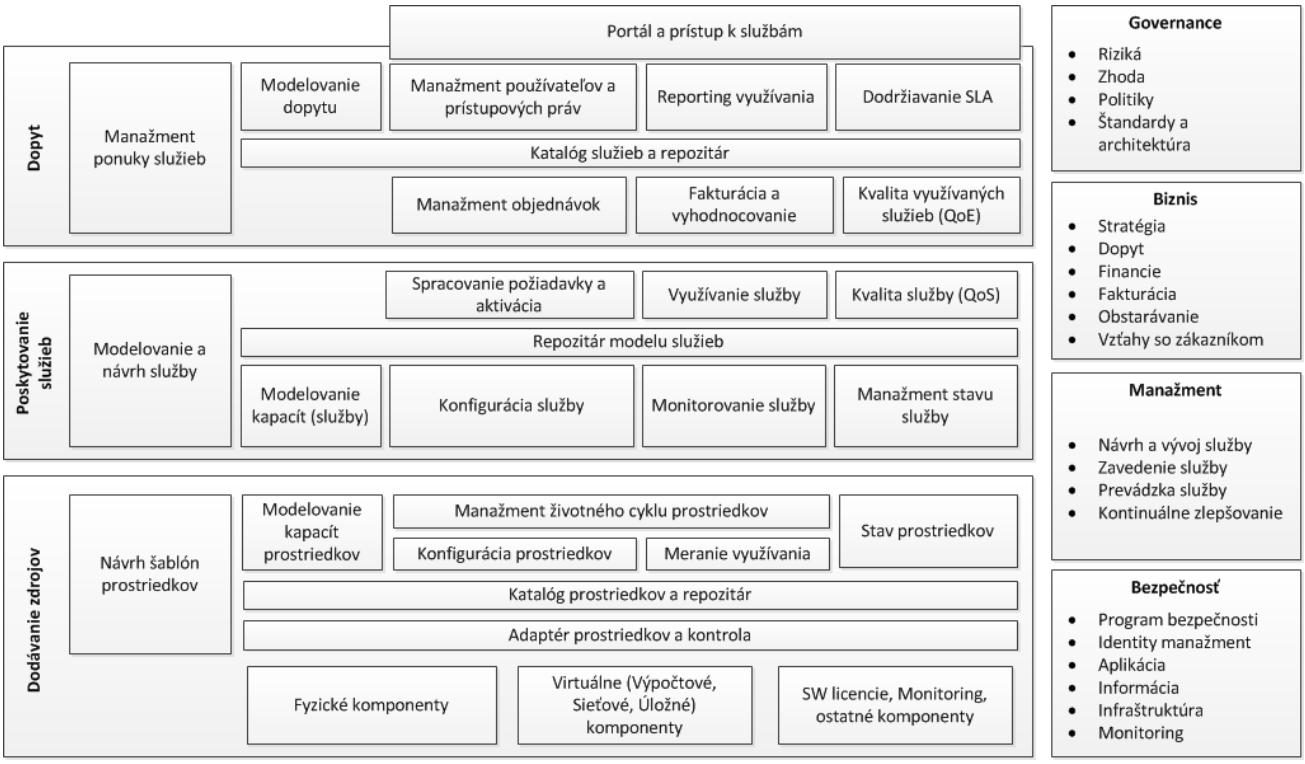
Meranie (Metering)

Poskytuje možnosť merania vlastností služby na určitej úrovni abstrakcie zodpovedajúcej určitému druhu služby (napr. uloženie údajov, spracovanie údajov, šírku pásma a aktívne užívateľské účty).

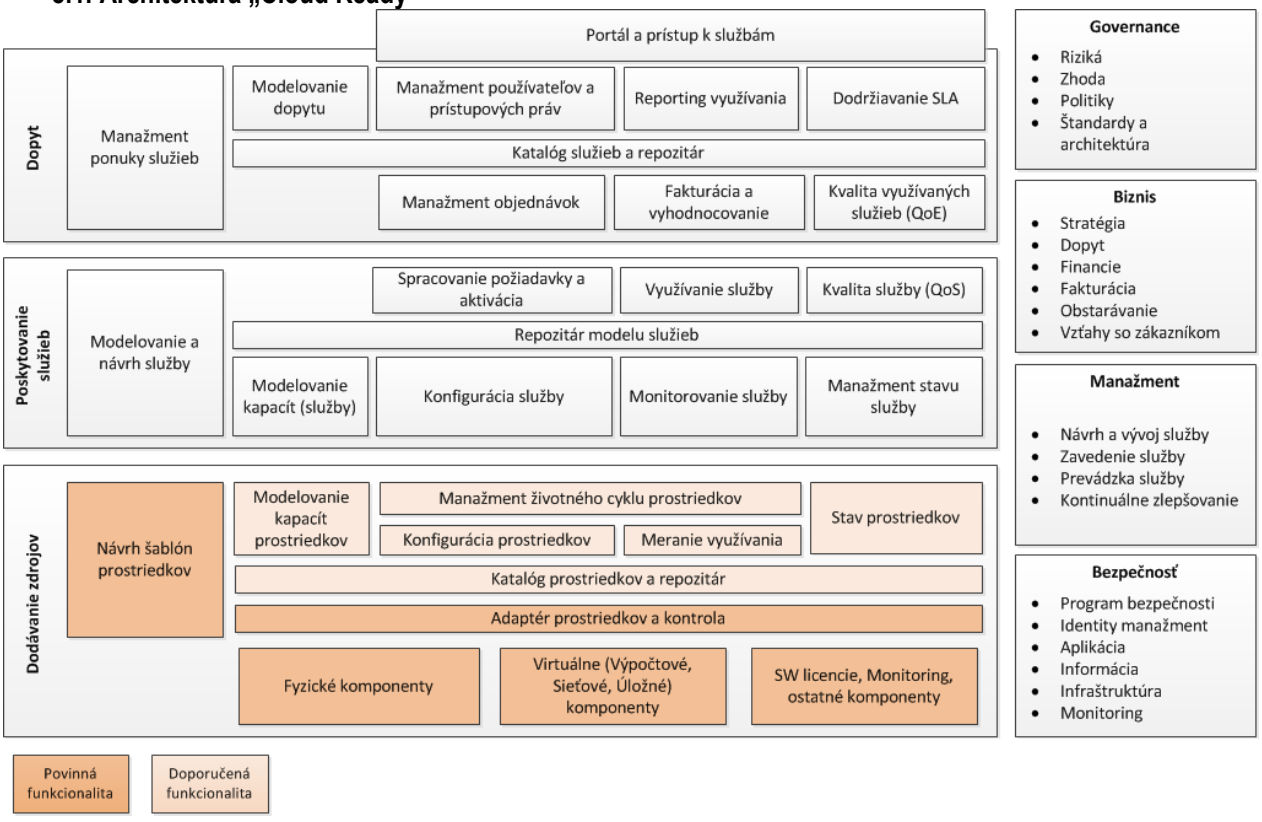
Požiadavky na úroveň služieb (SLA)

Zahŕňa definíciu SLA zmluvy (základná schéma s kvalitatívnymi parametrami služieb), SLA monitorovanie a vynucovanie SLA, podľa definovaných politík.

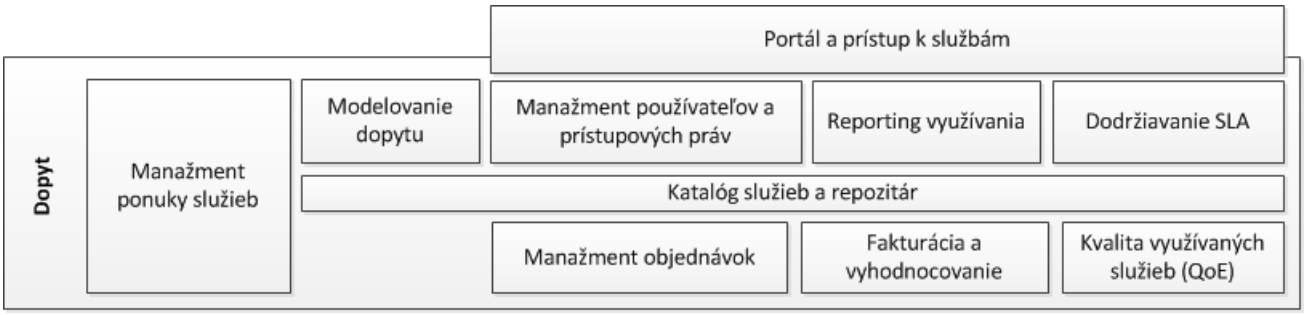
8. Príloha 2: Funkčná Referenčná Architektúra Goverment Cloud-u



8.1. Architektúra „Cloud Ready“



8.2 Vrstva dopytu



- Kombinuje jednu alebo viacero zákazníckych služieb/produktov do end-to-end služby
- Manažuje katalóg popisujúci služby, ktoré su dostupné pre koncových užívateľov
- Autentifikuje koncových užívateľov s cieľom určiť ich práva pre vytváranie a modifikovanie služieb.
- Povoľuje a iniciuje požiadavky na vytvorenie a modifikovanie služieb.
- Poskytuje fakturačné informácie pre služby a vysporiadania.
- Vizualizuje kvalitu využívaných služieb (Quality of Experience) zákazníka a dodržiavanie SLA.
- Manažuje mapovanie zákazníka a služby.

Komponenty

Portál a prístup k službám

Portál poskytuje zabezpečený "permission-based" mechanizmus prístupu a rozhrania (APIs) na prístup funkcií ktoré poskytuje Cloud prostredie.

Podporuje "role-based" prístup a potreby rôznych typov užívateľov.

Portál poskytuje prístup cez webové rozhranie.

Niektoré implementácie môžu poskytnúť tento prístup aj cez iné externé systémy.

Portál dovoľuje užívateľom služieb zabezpečený "permission-based" prístup na administráciu a kontrolu týchto služieb.

V závislosti na charakteristike služby, portál môže ale nemusí byť zapojený do využívanie služby. Napríklad ponuka "IaaS storage" môže mať nízkoúrovňové rozhrania na priamy prístup infraštruktúry prostredníctvom funkcie Service Access.

Manažment používateľov a prístupových práv

Poskytuje prístup, a autorizáciu užívateľov.

Využíva funkcie Manažmentu identít zahrnuté vo vrstve "Bezpečnosť"

Umožňuje riadenie životného cyklu užívateľa.

Využíva politiky na stanovenie spôsobilosti každej užívateľskej role.

V závislosti na prevedení, podporuje rôzne užívateľské role (napr. spotrebiteľské, administrátor, predajca) a "multi-tenancy" medzi užívateľmi (viacero zákazníkov)

Pre účely autorizácie, združuje politiky užívateľov založené na "role-based" prístupu k službám podnikových politík a pravidiel riadenia, ako je napríklad užívateľské usporiadanie a obmedzovanie zdrojov

Reporting využívania

Transformuje interné informácie o využití služieb do zákazníckych informácií.

Zachováva históriu využívania.

Môže vyvolať zmeny v kontrakte alebo upozornenia a proaktívne notifikácie.

Fakturácia a vyhodnocovanie

Kombinuje informácie o použití služby spotrebiteľom / zákazníkom s príslušnou cenou.

Založená na politikách, ktoré boli prerokované oceňovacích modelov a užívania služby (z Delivery vrstvy).

Prezentuje informácie ohodnotených použití do externého fakturačného systému (Invoicing – Business).

Poskytuje informácie ohodnotených použití pre funkcie urovnania a vyúčtovania s externými poskytovateľmi služieb a predajcami.

Podpora rôznych cenových modelov poskytovateľa: fixný poplatok, garantovaný poplatok, úrovňové poplatky, paušálny servisný poplatok, rozdelenie výnosov, a pod.

V závislosti na implementácii, podporuje rôzne účtovacie modely: chargeback, pre-paid, post-paid, trial, pay-per-use, a pod.

Poskytuje mechanizmy pre znemožnenie prístupu z dôvodov prekročenia limitov súm stanovených politikami pre zúčtovanie predplatného ("pre-paid") alebo riadenie úverového rizika (zabezpečené "Riadenie").

Dodržiavanie SLA (Service Level Agreement)

Manažment SLA je zodpovedný za agregáciu a reportovanie SLA medzi poskytovateľom služby a zákazníkmi ako aj poskytovateľom služby a dodávateľom

Priebežne, takmer v reálnom čase, počíta dodržiavanie SLA.

Poskytuje zabezpečený prístup k reportom ohľadne dohodnutých a zvalidovaných SLA.

Dodržiavanie SLA je zodpovedné za udržiavanie SLA manažment modelu.

Dodržiavanie SLA musí zdediť SLA informácie podľa toho ako "Manažment ponuky služieb" vytvára a obnovuje SLA podmienky.

Ako "Manažment objednávok" schváli nové SLA kontrakty, Dodržiavanie SLA musí začať verifikačný proces dodržiavania SLA.

Naviac k validácií zhody SLA pre služby poskytované zákazníkom, procesy môžu byť tiež použité na validáciu zhody SLA za služby poskytované dodávateľmi.

Validácia alebo odmietnutie sťažností zákazníkov ohľadne SLA.

Porovnáva externé monitorovanie SLA.

Manažment objednávok

Manažment objednávok prijíma objednávku cez portál alebo aplikačné rozhranie (API).

Potvrdzuje, že objednávka je správne a v súlade dohodnutými politikami (vrátane "entitlement").

Na základe katalógu služieb, objednávka je rozložená do prvkov služby.

Rozhoduje, ktoré prvky služby sú poskytované, ktorou konkrétnou vrstvou "Poskytovania služieb".

Smeruje požiadavky na prvky služieb do vrstvy "Poskytovania služieb", poskytuje status a iniciuje nápravu v prípade poruchy.

Používa katalóg služieb na rozhodnutie, ktoré služby môžu byť ponúknuté a udržiava informácie aké služby sú používané zákazníkom.

Kvalita využívaných služieb (Quality of Experience aka QoE)

Monitoring QoE je zodpovedný za poskytovanie pohľadu na to, ako tieto služby fungujú z perspektívy zákazníka.

QoE používa senzory, analytické nástroje a iné mechanizmy na monitorovanie služby end-to-end z pohľadu zákazníka.

Ak je kvalita služieb pod preddefinovanou úrovňou, nástroje QoE v spojení s nástrojmi QoS by mali umožniť identifikáciu jadra príčiny zhoršenia kvality.

QoE môže poskytovať informácie vyššiemu (externému) systému "Customer Experience Management" (Client Relationships – Business)

Katalóg služieb a repozitár

Katalóg služieb by mal obsahovať informácie:

- ponúkané služby a ich kompozície
- informácie o dohodnutých podmienkach (cena, SLA, a pod.) a špecifických prvkov služby, ktoré ju tvoria
- mapovanie nárokov (ktoré služby môžu byť objednané ktorými užívateľmi)
- užívateľom objednané služby

Ponuky služieb v katalógy môžu byť iniciované na vyžiadanie (nakonfigurované, ocenené a adekvátne monitorované).

Každá ponúkaná služba je spojená s SLA, ktoré popisuje rozsah a hranice pre splnenie konkrétnych potrieb zákazníkov.

- napríklad: politiky (OLA, prístup na službu, prevádzkový stav), objednávkové a požiadavkové procedúry

V katalógu služieb sú zadefinované obidve interné aj externé služby.

Manažment ponuky služieb

Manažment ponuky služieb podporuje proces zavádzania nových služieb, modifikácie a vyradzovanie existujúcich služieb v portfóliu aktívnych služieb.

Posúva tieto informácie do katalógu služieb.

Manažment ponuky služieb pomáha poskytovateľom Cloud služieb vyvíjať a komponovať ponuky služieb z jedného alebo viacerých prvkov služieb.

Definuje všetky aspekty služby z pohľadu zákazníka, o.i. SLA požiadavky, ocenenie, regionálna dostupnosť, a pod.

Modelovanie dopytu

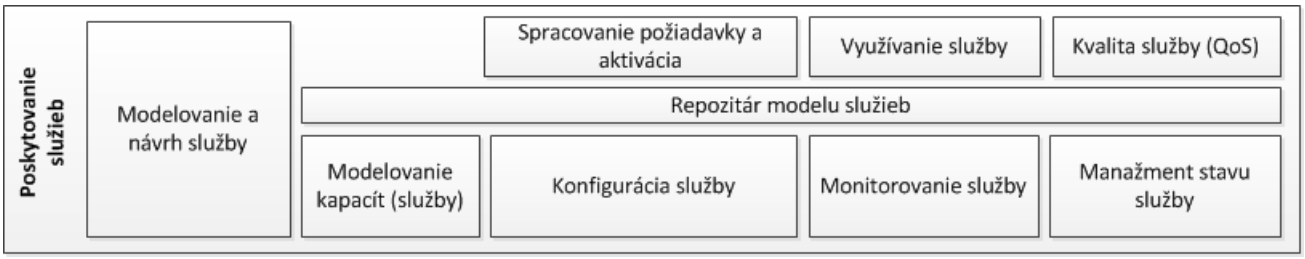
Definuje modely pre očakávaný dopyt nových a existujúcich ponúkaných služieb.

Spolu s modulom "Modelovania kapacít" (vrstva "Poskytovanie služieb"), predpovedá kedy dopyt prevýši súčasnú ponuku.

Prepája finančné modelovanie a obstarávanie (externá enterprise funkcia).

Napája sa na plánovanie kapacít.

9.1. Vrstva poskytovania služieb



- automatizuje a orchestruje kombinácie niekoľkých prvkov služieb (z jednej alebo viacerých vrstiev "Dodávanie zdrojov") do jednej služby
- vyberá najvhodnejšiu vrstvu "Dodávania zdrojov" (zahrňuje aj funkcionality "Cloud bursting")
    - na základe stanovených politík
    - na základe požiadavky vrstvy "Dopytu"
    - na základe dostupnosti vrstvy "Dodávania zdrojov"
- monitoruje a vypočítava využitie služby zákazníkom
- udržuje informácie o mapovaní služby k jej prvkom (fondy zdrojov vrstvy "Dodávanie zdrojov")

Komponenty

Spracovanie požiadavky a aktivácia

Spracováva servisné žiadosti o interne poskytovaných službách.

Je rozhraním do vrstvy "Dopyt" (Manažment objednávok), prijíma požiadavky na služby a procesuje ich na základe SLA politík, dostupnosti a výkonnosti zdrojov a konfiguračného modelu služieb.

Keď viaceré vrstvy "Dodávania zdrojov" spĺňajú kritéria na vybavenie požiadavky, použije politiky na zvolenie vrstvy "Dodávania zdrojov" ktorá sa využije.

Niektoré politiky môžu byť viazané na existujúce regulácie.

Orchestruje aktiváciu a deaktiváciu, nastavenie použitia a zapísanie stavov služby do repozitára.

Iniciuje rollback alebo iné nápravné kompenzácie pri zlyhaní.

Aktivácia služby sa môže líšiť podľa typu služby.

Obsahuje workflow, ktorý synchronizuje nasadzovanie všetkých komponentov služby s transakčnou konzistenciou.

Generuje požiadavky na príslušnú vrstvu "Dodávania zdrojov" pre nasadzovanie prvkov služby ako je potrebné.

Nakonfiguruje použitie a zaisťuje funkcie na monitorovanie služby.

Využívanie služby

Zbiera záznamy o využívaní a meraní (CDR. XDR, a pod.) a spracováva ich pre každého zákazníka a pre každý záznam o využití služby,

Spracovanie môže byť implementované dávkovo alebo v reálnom čase.

Okrem poskytovania fakturácie a hodnotenia, môže tiež poskytovať informácie pre manažment rizík a "fraud" detekcie.

V závislosti na implementácii môže ukladať informácie o využití služieb pre ďalšie podrobné analýzy (pre manažment dopytu, CRM a pod.)

Kvalita služby (Quality of Service aka QoS)

QoS sa prepája s monitorovaním služieb pre získavanie dát o stave a výkone služieb a prostriedkov pre priebežný SLA a dynamické alokovanie zdrojov.

QoS spolu s QoE ("Kvalita využívaných služieb") poskytuje vstupy pre zákazníkov dojem.

Poskytuje reporting ako z histórie tak aj v reálnom čase o prevádzkových servisných úrovniach a poskytuje dáta pre zákazníkovu SLA.

Konfigurácia služby

Definuje ako sú prvky služby kombinované pre poskytnutie v rámci vrstvy "Dodávania zdrojov" (na základe informácií v repozitári modelu služby).

Špecifikuje atribúty služby ako napr. IP adresa (ktoré nie sú pod kontrolou vrstvy "Dodávania zdrojov", alebo nie sú definované v objednávke) a priraďuje ich k inštanciám služby.

Príjma špecifickú konfiguráciu z prostriedkov nasadených vo vrstve "Dodávania zdrojov".

Poskytuje spojenie medzi službami vrstvy "Dopyt" a zdrojmi vrstvy "Dodávania zdrojov", ktoré implementujú služby.

Poskytuje informácie požadované pre nasadenie potrebných prostriedkov pre poskytovanie služieb zákazníkovi.

Konfigurácia môže byť zmenená bez aktivácie.

Monitorovanie služby

Konfigurácia monitorovania služieb nasledujúca za aktiváciou a aktualizáciou služby.

Zhromažďovanie udalostí v reálnom čase a dát o výkone pre manažment stavu služby ako aj agregovanie do QoS funkcie pre priebežný SLA a dynamické alokovanie prostriedkov.

Ak je vrstva "Dodávania zdrojov" nadmerne preťažená, môže podať žiadosť do "Spracovania Požiadaviek a Aktivácií" pre donasadenie služieb iných vrstiev "Dodávania zdrojov".

Aktualizácia repozitára modelu služieb v reálnom čase.

Manažment stavu služby

Zbiera udalosti na úrovni prostriedkov a eskaluje ich do servisných incidentov, ak je to relevantné.

Udržuje prehľad o stave služby.

Ukladá udalosti na úrovni služby.

Koreluje udalosti na úrovni služby a eskaluje ich do servisných incidentov, ak je to relevantné.

Iniciuje incident pre Service Desk (trouble ticketing).

Repozitár modelu služieb

Model služby obsahuje obidva druhy informácií ako na úrovni typu, tak aj samotnej inštancii:

- definuje hierarchiu služieb
- mapovanie medzi zákazníckymi službami a potrebnými prostriedkami
- konfiguračné šablóny
- workflows pre aktiváciu a deaktiváciu
- atribúty služby
- zachycuje stavy služby v reálnom čase

Modelovanie a návrh služby

Špecifikácia služby, definujúca ako je služba naimplementovaná.

Umožňuje definíciu informácií potrebných do "Repozitára modelu služieb".

Definuje atribúty typu služby a identifikuje kde sa jej inštancia dostane hodnotu.

Definuje výnimky.

Návrh šablón služieb a workflow pre automatizáciu.

Manažment pre revíziu a uvoľňovanie služby ("service release").

Modelovanie kapacít (služby)

Prijíma prognózy a trendy prevádzkových kapacitných požiadaviek (z vrstvy "Dodávania zdrojov").

Od vrstiev "Dodávania zdrojov" prijíma zásoby prostriedkov a ich projekcie.

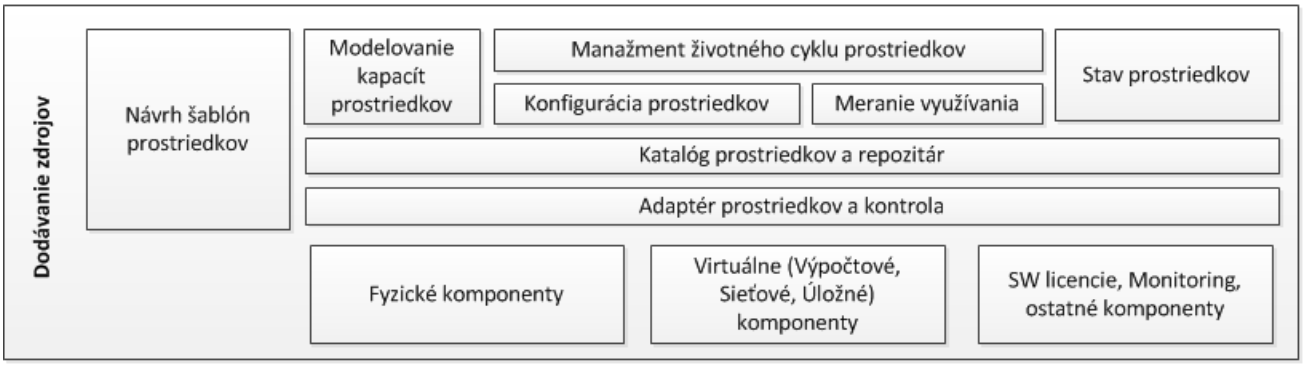
Modeluje či dopyt môže byť dodaný pomocou vrstiev "Dodávania zdrojov".

Prepája sa s sekciou "Riadenia" pre podporu rozhodovania, ako riešiť súčasné a budúce nedostatky.

Prepája sa s Repozitárom Modelu Služieb pre priebežné hodnotenie kapacít.

Prepája sa so službou modelovanie kapacít v vrstve "Dodávania zdrojov".

10.1.Vrstva dodávania zdrojov



- Izoluje vrstvu poskytovania od zdrojov pomocou zákazníckych abstrakcií služieb, prípadne kombináciou viacerých heterogénnych zdrojov do jednej abstrakcie.
- Poskytuje potrebné riadenie a orchestráciu na zabezpečenie poskytnutia prostriedkov pre požadovanú službu zákazníkovi.
- Optimalizuje využitie prostriedkov v rámci spoločného fondu (resource pool).
- Monitoruje využitie prostriedkov generujúc dáta o využívaní, ktoré môžu byť potenciálne fakturované.
- Zaisťuje normálny stav manažovaných prostriedkov.
- Udržuje katalóg fondu prostriedkov (resource pool catalog) popisujúci fyzický a logický repozitár prostriedkov.

Komponenty

Návrh šablón prostriedkov

Zodpovedný za návrh prostriedkov infraštruktúry a modifikácie špecifických typov fondov prostriedkov na základe služieb využívaných zákazníkmi, ktoré sú definované v moduloch "Modelovanie a návrh služby", "Konfigurácia služby", "Modelovanie kapacít služby" v rámci vrstvy "Poskytovanie služieb".

Prepája sa s modulmi "Modelovanie a návrh služby", "Konfigurácia služby", "Modelovanie kapacít služby" v rámci vrstvy "Poskytovanie služieb".

Návrh pracovných postupov ("workflow") pre manažment fondov prostriedkov vrátane konfigurácie prostriedkov, nasadzovanie, manažment zaťaženia a automatizácie špecifických alebo všeobecných služieb využívaných zákazníkmi.

Návrh "Katalógu prostriedkov a repozitára".

Návrh metrík manažmentu fondu prostriedkov pre monitorovanie ich stavu.

Modelovanie kapacít prostriedkov

Prepája sa s modulom "Modelovanie kapacít služieb" z vrstvy "Poskytovania služieb" pre prognózovanie spotreby zdrojov

Reporting kapacít a výkonností fondov zdrojov v reálnom čase alebo v histórií. Koordinácia komponentov vrstvy "Dodávania zdrojov" v rámci konfigurácií zdrojov, manažmentu záťaže a monitorovania pre modelovanie požiadavky na dodávku. Mapovanie informácií požiadaviek na prostriedky s dostupnými zdrojmi v "Katalógu prostriedkov a repozitári". Previazaný s doménou "Riadenia" pre obstarávanie dodatočných prostriedkov ak potrebné.

Manažment životného cyklu prostriedkov

Prijíma požiadavky na kapacity a výkon z "Modelovanie kapacít prostriedkov" (Resource Capacity Modelling) a "Návrh šablón prostriedkov" (Template Design).

Určuje potrebný počet a typy fondov prostriedkov na základe požiadavky na konfiguráciu kapacity služby.

Manažuje spotrebu fondu prostriedkov (resource pool) a modul pre meranie využitia.

Prijíma požiadavky z vrstvy "Poskytovania služieb" a inteligentne alokuje prostriedky.

Prijíma informácie o dostupnosti nových prostriedkov a komunikuje ich do vrstvy "Poskytovania služieb".

Orchestruje komponenty fondov prostriedkov pre podporu záťaže na službu a manažuje rozdelenie záťaže v reálnom čase s preddefinovanou workflow logikou a algoritmom

Pre monitorovanie zdrojov a meranie využitia reportuje Manažérovi fondu prostriedkov zmeny v nastaveniach prostriedkov v dôsledku dynamického manažmentu prostriedkov

Konfigurácia prostriedkov

Od manažéra fondu zdrojov prijíma informácie o kapacitných konfiguráciách prostriedkov.

Mapovanie informácií o konfiguráciách prostriedkov do "Katalógu prostriedkov a repozitára".

Konfiguruje a nasadzuje prostriedky pomocou abstraktnej vrstvy manažéra poskytovateľa prostriedkov (Resource Provider Manager).

Meranie využívania

Pomocou manažéra fondu prostriedkov sleduje zmeny spotreby a používania komponentov fondu prostriedkov špecifických pre danú službu alebo používateľa

Modulom "Využívania služby" a "Monitorovania služby" vrstvy "Poskytovania služieb" poskytuje reporty využitia komponentov fondu prostriedkov.

Monitoruje dostupnosť a úroveň spotreby komponentov zdrojov prostriedkov, informuje manažéra poskytovateľa prostriedkov, ak fondy prostriedkov sú alebo budú preťažené.

Modulu "Využívania služby" vrstvy "Poskytovania služieb" poskytuje informácie o nameranom využívaní zdroja prostriedkov

Informuje moduly "Monitorovania služby" a "Kvalita služby" vrstvy "Poskytovania služieb", ako aj manažéra poskytovateľa prostriedkov.

Doménam "Riadenie" a "Bezpečnosť" nahlasuje bezpečnostné hrozby na úrovni komponentov zdroja prostriedkov

Stav prostriedkov

Vrstve "Poskytovania služieb" poskytuje informácie o chybách v rámci fondu zdrojov, ktoré môžu potenciálne ovplyvniť poskytovanie služieb ("Manažment stavu služby").

Pomocou manažérom fondu prostriedkov môže byť vyvolaná, chybovým stavom prostriedku, autonómna oprava.

Monitoruje chybové stavy komponentov fondu prostriedkov a v prípade takejto chyby iniciuje "failover" proces.

V reálnom čase udržuje agregované reporty manažmentu udalostí ohľadne dostupnosti komponentov zdroju prostriedkov a zlyhania hardvéru pomocou manažéra poskytovateľa prostriedkov ("Resource Provider Manager")

Katalóg prostriedkov a repozitár

Unifikované informácie komponentov prostriedkov obsahujúce typy kompozícií fondov zdrojov (resource pool) vrstvy "Dodávania zdrojov".

Aktualizácie služieb v reálnom čase zachytené modulmi pre modelovanie kapacít a stavov prostriedkov.

Manažér dynamického zaťaženia používa v reálnom čase stav prostriedkov k vyváženiu zaťaženia v rámci fondu prostriedkov (resource pool).

Mapovanie modelov poskytnutia služby na komponenty fondu prostriedkov (resource pool).

Softvérové licencie.

Adaptér prostriedkov a kontrola

Objavovanie komponentov fondu prostriedkov (servre, úložiská, sieť, softvér).

Poskytuje abstraktnú vrstvu na konfiguráciu, nasadzovanie, manažovanie a monitorovanie fyzických komponentov fondu prostriedkov.

Modulom katalógu fondu zdrojov, merania využitia a stavu prostriedkov, poskytuje aktualizovaný stav a informácie o využitia komponentov hardvéru a softvéru v reálnom čase

11.1."Enterprise" Funkcionality - funkcionality prechádzajúce cez všetky vrstvy

- Táto rovina obsahuje celkové "enterprise" funkcionality, ktoré poskytujú bežné operácie a manažment ako pre Cloud tak aj pre tradičné non-Cloud prostredia.
- Niektoré funkcie majú Cloud špecifické komponenty (umiestnené v modrej rovine) a všeobecnejšie komponenty, ktoré poskytujú celkovú funkcionalitu požadovanú pre Cloud prostredia.
- Táto rovina sa zameriava na štyri kľúčové oblasti:
    - Riadenie rizík, dodržiavanie predpisov, politík, noriem, architektúry a pod.
    - Biznis manažment vrátane stratégie, dopytu, financie, fakturácie, obstarávania a manažment vzťahov so zákazníkmi.
    - Integrovaný manažment Cloud a tradičného non-Cloud prostredia.
    - Bezpečnosť vrátane manažmentu identít a bezpečnosti aplikácie, informácií a infraštruktúry

Domény

Governance

Riadenie zaisťuje, že investície do IT vytvárajú biznis hodnotu, a zmierňujú riziká ktoré sú s ňou spojené. Toto sa dosahuje zavedením organizačnej štruktúry s dobre definovanými rolami a zodpovednosťami na úrovni informácií, biznis procesov, aplikácií, infraštruktúry.

Riadenie zahrňuje:

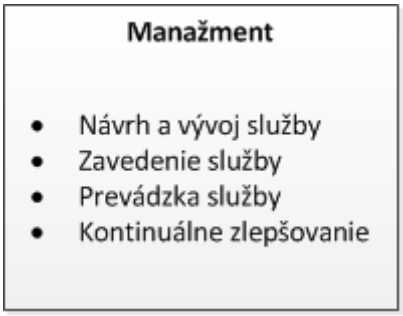
- Rámec politík definujúci rozhrania, procesy a procedúry, role a zodpovednosti, a pod.
- Rámec plnenia povinností, definujúci cestovnú mapu úrovni dospelosti (Maturity Level Roadmap) a kontroly cieľov v rámci životného cyklu
- Štandardy a architektúru definujúce architektonické riadenie vrátane Bezpečnosti, kontinuity služieb, dostupnosti a kapacít.
- Manažment rizík: definície kontroly a sledovania

Biznis

Biznis sekcia sa zameriava na biznis manažment enterprise prostredia (Cloud & non-Cloud):

- Stratégia určuje ako by sa mali vyvíjať celé IT enteprise portfólio tak, aby zodpovedalo potrebám organizácii a ako sú získavané.
- Dopyt stanovuje projektovaný dopyt pre produkty a služby, a odhaduje zdroje potrebné pre poskytnutie produktu / služby s vhodným QoE.
- Financie stanovujú, ako môže byť produkt / služba získaná a poskytnutá ekonomicky najefektívnejším spôsobom, a v prípade účtovníctva stanovuje príslušnú cenu / náklad.
- Fakturácia spravuje procesy fakturácie v prípade účtovníctva.
- Obstarávanie sa prepája s externými poskytovateľmi, vyjednáva kontrakty (vrátane SLA), posiela objednávky a manažuje fakturáciu s dodávateľmi.
- Sekcia klientskych vzťahov udržuje zákazníkove informácie, vyjednáva SLA, vybavuje sťažnosti a ďalšie interakcie s klientmi.

Manažment

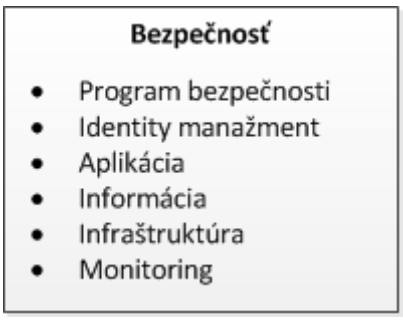


Manažment spracováva operácie v enterprise prostredí (Cloud and non-Cloud) a zahŕňa:

- Návrh a vývoj služby a procesov. Zahŕňa manažment portfólia služieb a ich životného cyklu.
- Prechod služieb prináša nové a pozmenené služby do prevádzky.
- Servisné operácie sa zameriavajú na prevádzkové potreby enteprise prostredia, vrátane manažmentu udalostí a incidentov, riešenie problémov, manažment servisných požiadaviek a pod.
- Kontinuálne zlepšovanie analyzuje úspech a zlyhania pre pochopenia ako zlepšiť procesy a procedúry. Zaoberá sa taktiež samotným prostredím a možnosťami jeho vylepšenia.

Manažment vo veľkej miere využíva ITIL v3.

Bezpečnosť



Bezpečnosť sa zameriava na profil manažmentu rizík v kontexte biznisu. Je založený na bezpečnostný program, ktorý definuje bezpečnostnú kontrolu a mechanizmu, aby bola čo najlepšie zabezpečené enteprise prostredie (Cloud and non-Cloud):

- Podpora "multi-tenancy" izolácie - zhora nadol
- Manažment kompletného životného cyklu identity
- Celkové end-to-end zabezpečenie aplikácie (napr. bezpečné SDLC).
- Jasné politiky bezpečnosti informácií a ich presadzovanie.
- Monitorovanie bezpečnosti a automatické reakcie v celom enterprise prostredí.
- Zaisťuje validáciu dodržiavania bezpečnosti v prostredí
- Celkové end-to-end zabezpečenie infraštruktúry vrátane IDSP a manažmentu ohrozenia (Threat Management)

9. Príloha 3: IaaS služby

12.1.Služba úložných zdrojov (Storage as a Service)

Služba spočíva v používaní úložnej kapacity, ktorá je meraná a odberateľovi služby účtovaná podľa vopred dohodnutých kritérií.

Samotná HW a SW infraštruktúra, ktorá je potrebná pre prevádzku služby sa skladá z pevných diskov, radičov, ich rozhraní, prepojovacej siete, súvisiacich ovládačov, softvérových nástrojov a ďalších komponentov. Všetky spomínané časti v rámci riešenia ale sú plne v správe prevádzkovateľa služby a sú pre odberateľa transparentné.

Dôležitým aspektom služby je vysoká dostupnosť, kde je zabezpečená prevádzka bez výpadku, aj v prípade čiastočného alebo úplného zlyhania niektorého z komponentov, napájania, konektivity a pod.

Tabuľka IaaS.Storage.1: Povinné parametre "Služby úložných zdrojov"

Parameter	Popis Parametra
Kapacita	Kapacita úložného priestoru (GB)
Rýchlosť	Rýchlosť prístupu k dátam (ms)
Výkonnosť	Počet I/O operácií za sekundu (IOPS)
Dostupnosť	Podieľ času v ktorom je služba funkčná (%)

Vzhľadom na veľké množstvo vzájomných kombinácií parametrov služby úložných zdrojov, nie je bežné jej poskytovanie vo všetkých variantoch. Riešením je definovaný katalóg niekoľkých rôznych úrovní pokrývajúcich najčastejšie využitie odberateľov.

Tabuľka IaaS.Storage.2: Úrovne "Služby úložných zdrojov"

Parameter	Popis Parametra	Úroveň 1	Úroveň 2	Úroveň 3
Rýchlosť	Rýchlosť prístupu k dátam (ms)	< 8 ms	7 – 14 ms	12 – 30 ms
Výkonnosť	Počet I/O operácií za sekundu (IOPS)	5000+	3500 - 5000	1500 - 3500
Dostupnosť	Podiel času v ktorom je služba funkčná (%)	99.999	99.99	98
Použitie		Aplikačné dáta	Dáta užívateľov	Archív

13.1. Služba výpočtových zdrojov (Compute)

"Služba výpočtových zdrojov" poskytuje v rámci IaaS výpočtové zdroje, ktoré sú využívané pre beh OS v Cloude. Výpočtové zdroje môžu byť dynamicky poskytované a konfigurované podľa aktuálnej potreby.

Ku každému virtuálnemu serveru je možné pripojiť úložné zdroje podľa potreby.

Všetky ponúkané výpočtové zdroje sú garantované.
VPU (Virtual Procesor Unit) jednotka je definovaná ako výpočtový výkon jedného core procesora schopného dosiahnuť výkon min. 41,5 bodov podľa benchmarku SPECint_base2006 [1]. (Pozn.: Hodnota ktorá dnes odpovedá CPU 2.0 GHz Intel Xeon E5-2650)

HDD je poskytované z diskového poľa v Úrovni 2. definovanej v "Službe úložných zdrojov".

Na výber gCloud poskytuje základné HW konfigurácie virtuálnych serverov. Tieto sú rozdelené do skupín a dosahujú úroveň SLA minimálne 99.99%:

[1] Hodnota vyjadrujúca výkon CPU podľa metodiky nezávislého štandardizovaného testovania ***The Standard Performance Evaluation Corporation (SPEC).***

Tabuľka IaaS.Compute.1: Úrovne výpočtových zdrojov.

1) Štandardné

názov	VPU	Mem v GB	HDD v GB
malá	2	4	80
stredná	6	8	160
veľká	8	12	250

2) Výkonné

názov	VPU	Mem v GB	HDD v GB
malá	12	8	300
stredná	16	12	500
veľká	20	16	1000

3) Pamäťovo náročné

názov	VPU	Mem v GB	HDD v GB
stredná	16	32	850
veľká	24	64	1200

4) Fond prostriedkov (virtuálne dátove centrum)
Fond prostriedkov (Resource Pool) je definovaný sumárnymi hodnotami VPU (core), RAM (GB), úložné zdroje (GB, Úroveň podľa špecifikácie "Služby úložných zdrojov").

"Služba výpočtových zdrojov" môže byt účtovaná fixným poplatkom v mesačnom platobnom cykle, alebo iba za čas ktorý je virtuálny server zapnutý, s najmenšou meranou časovou jednotkou 1 hodina.

14.1.Manažment Cloud služieb

Zahŕňa nevyhnutné funkcie, ktoré sú potrebné pre správu a prevádzku IaaS služieb.

Odporúčané funkcie

Katalóg prostriedkov a repozitár: umožňuje nastavovanie a správu prostriedkov
Konfigurácia prostriedkov: zabezpečuje automatické nasadzovanie Cloud systémov vytvorených z dostupných zdrojov na základe požadovaných služieb
Meranie využívania: umožňuje meranie na úrovni abstrakcie zodpovedajúcej typu služby (napr. využívanie slu6by úložných zdrojov, výpočtových zdrojov, prenosovej kapacity aktívnymi používateľskými účtami)
Manažment životného cyklu prostriedkov: vyhľadáva a monitoruje virtuálne zdroje, sleduje prevádzku Cloudu, výskyt udalostí a generuje prevádzkové reporty
Manažment stavu služby: monitoruje QoS parametre podľa dohodnutého SLA kontraktu a umožňuje vynucovanie SLA na základe definovaných politík

Interoperabilita služieb a prenositeľnosť systémov

Interoperabilita služieb umožní konzumentom Cloud služieb využívať služby naprieč viacerými cloudmi cez unifikované používateľské rozhranie.
Prenositeľnosť systémov umožní migráciu stopnutej inštancie virtuálnej mašiny alebo obrazu virtuálnej mašiny z aktuálne využívaného Cloudu do iného Cloudu (príp. aj s rozdielnou virtualizačnou technológiou).

Každé cloudové riešenie by malo využívať mechanizmy, technológie a formáty podporujúce interoperabilitu služieb a prenositeľnosť systémov.

15.1.Služba zálohovania (Backup as a service)

Zálohovanie, ako poskytovaná Cloud služba je braná ako doplnok k službe "Výpočtových zdrojov", t.j. k výpočtovému výkonu. Pri službe "Výpočtových zdrojov" sa a priori predpokladá jej beh nad diskovým priestorom s ochranou pred výpadkom niektorého fyzického disku. „Služba zálohovania" je posunutá o úroveň vyššie a zabezpečuje, pokiaľ si zákazník objedná, možnosť konzistentných záloh a obnov dát v samotnom operačnom systéme.

Vykonanie manuálnej zálohy alebo obnovy dát, ako aj nastavenia automatizovaných činností je pri "Službe zálohovania" v zodpovednosti Konzumenta. Znamená to, že nastavenie a dodržanie hodnôt RPO (recovery point objective) a RTO (recovery time objective) je v zodpovednosti Konzumenta. Prakticky, podľa zvolenia RPO a RTO si následne Konzument vyberá úrovne služieb "Služba úložných zdrojov " a "Služby zálohovania".

Tabuľka IaaS.Backup.1: Definujeme 3 rôzne úrovne prístupu a konzistentnosti dát:

Úroveň	Popis
Úroveň 1.	Záloha/obnova dát na úrovni obrazu disku, resp. klonu disku virtuálneho servera.
Úroveň 2.	Záloha/obnova dát na úrovni súborov v operačnom systéme.
Úroveň 3.	Záloha/obnova dát na úrovni natívnych prostriedkov relačných databáz pri zachovaní plnej dátovej konzistencie.

Pre Úroveň 1. platí, že nemusí, ale môže, garantovať konzistenciu dát ani na úrovni súborov ani databáz. Používa sa pri zálohách systémov, v ktorých sa údaje nemenia, typicky statické front end web servery a pod., pri ktorých je podstatná prvotná konfigurácia a funkčnosť ale do ktorých je možné z redakčného systému dáta kedykoľvek nanovo umiestniť. Úroveň 2. je klasická záloha súborov a adresárov v súborových systémoch na úrovni operačného systému. Úroveň 3. je sofistikované zálohovanie cez API databázových systémov. Tento typ, napriek malému zastúpeniu generuje najväčší objem zálohovaných dát.

K týmto trom úrovniam sa pridáva základný parameter a tým je celkový rezervovaný priestor pre zálohy, pre ktorý sa navyše definuje v rôznych úrovniach rýchlosti prístup k zálohám (t.j. nie čas obnovy, ale čas dostupnosti záloh).

Tabuľka IaaS.Backup.2: Úrovne dostupnosti záloh:

Úroveň	Popis
Úroveň 1.	Dostupnosť okamžite
Úroveň 2.	Dostupnosť v minútach
Úroveň 3.	Dostupnosť v hodinách

Požiadavka na úrovne dostupnosti záloh sa prakticky rovná definovaniu možností ich umiestnenia. Úroveň 1. znamená, že okamžite po iniciovaní obnovy dát sa dáta začnú obnovovať a celá obnova je kontinuálna. Úroveň č.2 v svojej definícii predpokladá, že dáta sú uložené na páskach, niekoľko minút môže trvať kým sa príslušná páska nájde, presunie do mechaniky, pretočí na konkrétny blok a začne čítať. Taktiež je nutné si uvedomiť, že záloha môže byť rozložená na rôznych páskach, takže celkový čas obnovy môže byť nezanedbateľne vyšší ako pri Úrovni č.1. Posledná Úroveň č.3 zodpovedá stavu, keď potrebné pásky na obnovu dát sa v páskovej knižnici už nenachádzajú a je potrebné ich manuálne vyhľadať, dopraviť a vložiť do páskovej knižnice.