Požadavky na zápis aplikací formou služby do katalogu cloud computingu s ohledem na nuance modelů SaaS a PaaS

verze 2.0; 20. 11. 2024

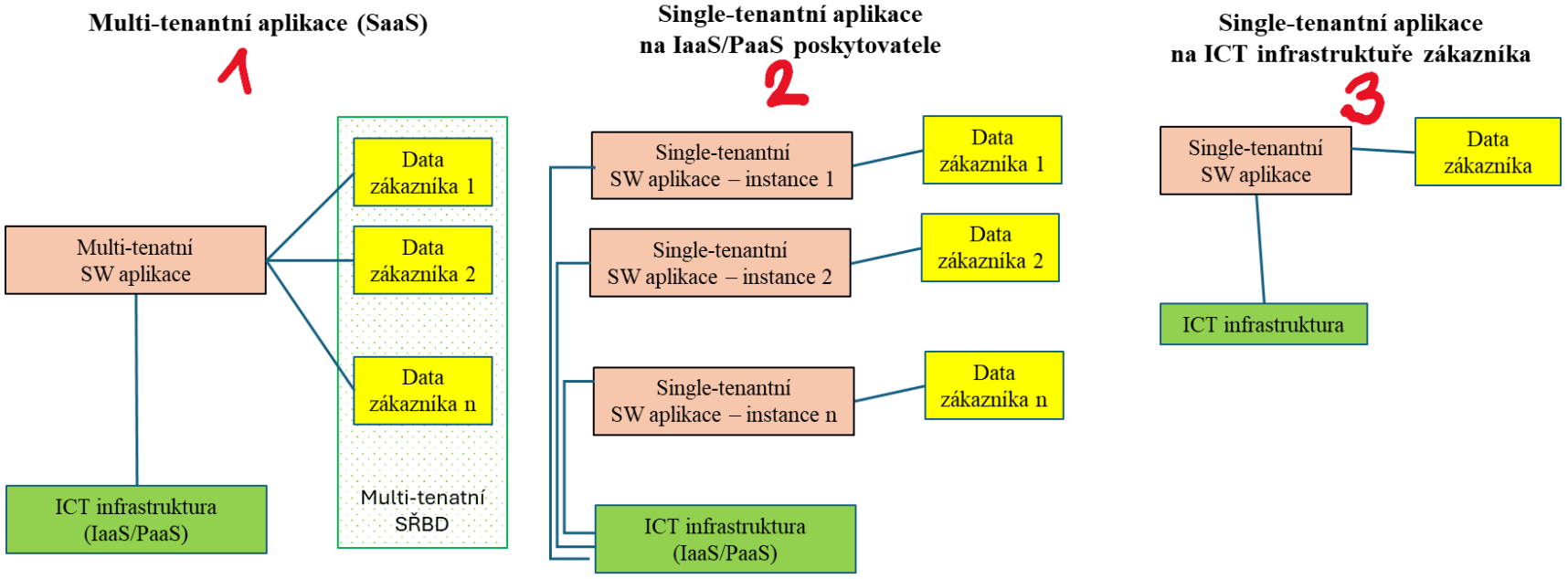
Obsah

1. Účel dokumentu

V období říjen-listopad 2024 obdržela Digitální a informační agentura několik dotazů ze strany poskytovatelů cloud computingu, které se týkaly upřesnění povinnosti zápisu jak vlastní aplikace poskytované formou služby, tak i jejích podpůrných platformních komponent. Cílem tohoto dokumentu je vysvětlit nuance, které mohou nastat z hlediska architektury a využívání sdílených služeb, a dále upřesnit pravidla, která se uplatní při zápisu služeb, využívajících dané architektury do katalogu cloud computingu (dále jen „CC“, viz také seznam použitých zkratek v závěru tohoto dokumentu).

2. Modely dodávky a provozu aplikací a jejich vztah k definici cloud computingu v ZoISVS

V prvním přiblížení lze rozlišit architekturu a způsob zajištění provozu aplikací: (1) čistě multi-tenantní aplikace, (2) single-tenantní aplikace na sdílené cloudové platformě IaaS a případně i PaaS, a (3) single-tenantní aplikace na vyhrazené ICT infrastruktuře zákazníka (on-premise nebo tradiční outsourcing).



Definice cloud computingu v ZoISVS přitom nerozlišuje, na které architektonické úrovni dochází k dálkovému přístupu ke „sdílenému technickému nebo programovému prostředku“. Viz definice v ZoISVS, § 2 odst. (2) písm. b): *cloud computingem (se rozumí) způsob zajištění provozu informačního systému veřejné správy nebo jeho části prostřednictvím dálkového přístupu k sdílenému technickému nebo programovému prostředku, který je zpřístupněný poskytovatelem cloud computingu a nastavitelný správcem informačního systému veřejné správy*.

Vysvětlení rozsahu uplatnění této definice již bylo publikováno v sekci Otázky a odpovědi (otázka č. 1) na webu DIA[1]. Zde vyvozené závěry:

(i) umístí-li zákazník (OVS) vlastní technické prostředky, nebo pronajme-li si zákazník (OVS) dedikované technické prostředky (tzn. prostředky sloužící výhradně tomuto zákazníkovi) umístěné v datovém centru poskytovatele (servery, disková pole atd.) a přístup k těmto prostředkům se realizuje privátním síťovým připojením, **pak se jedná o využití klasického outsourcingu. Nejedná se tedy o cloud computing,**

(ii) umístí-li zákazník vlastní technické prostředky, nebo pronajme-li si zákazník dedikované technické prostředky (servery, disková pole atd.) a přístup k těmto prostředkům se realizuje připojením, ve kterém zákazník využívá sdílené služby na 4. nebo vyšší vrstvě OSI, **pak se jedná o cloud computing (třída IaaS nebo PaaS),**

(iii) pronajme-li si zákazník službu sdílené infrastruktury (servery, disková pole atd.) a na ní umístí svůj platformní software (operační systém, databázový systém apod.) a na něm provozuje svůj ISVS, pak se **jedná o cloud computing (třída IaaS),**

(iv) pronajme-li si zákazník službu sdílené platformy (tj. hardwarové zdroje, vývojové, integrační a provozní prostředí aplikací (tj. včetně operačního systému, databázového systému, middleware apod.) a na ní provozuje svůj ISVS, pak se **jedná o cloud computing (třída PaaS),**

(v) pronajme-li si zákazník službu sdílené aplikace (např. e-mailový server, spisovou službu, ERP, HR), tj. pronajatá aplikace realizuje ISVS, pak se **jedná o cloud computing (třída SaaS).**

[1] Viz otázka 1 (https://www.dia.gov.cz/oha/egovernment-cloud/otazky-a-odpovedi/)

V druhém až pátém případě musí být poskytovatel cloud computingu a jeho služby zapsány v katalogu cloud computingu tak, jak stanoví Hlava VI ZoISVS. Zápis poskytovatele a nabídky CC je dle ZoISVS obligatorní podmínkou toho, aby orgán veřejné správy mohl tyto služby využívat.

V následujícím textu jsou dále upřesněny architektonické varianty využití podpůrného CC, které mohou v praxi nastat při poskytování aplikace formou služby. Jde zejména o rozlišení multi-tenantního nebo single-tenantního využití samotné aplikace i jejího podpůrného CC (číslování variant níže se vztahuje k obrázku na str. 2):

1. **Multi-tenantní aplikace provozovaná na IaaS/PaaS, tedy aplikace třídy SaaS:** Jedná se o kompletně sdílené prostředí, kde více zákazníků využívá současně jednu instanci aplikace. V čistě multi-tenantním modelu jsou taktéž všechny podpůrné služby (zejména systém řízení báze dat SŘBD) využívány multi-tenantně, tedy jako sdílené služby PaaS a IaaS. [1] [3] [4] [5]

2. **Single-tenantní aplikace provozovaná na IaaS/PaaS:** Každý zákazník má vlastní instanci aplikace běžící na sdíleném prostředí IaaS/PaaS. Poslední praxe však ukazuje, že **v této variantě mohou nastat nuance** – zdali jsou všechny platformní komponenty využívány skutečně single-tenantně, nebo jestli zde může docházet ke sdílení některých komponent různými tenanty (OVS). Varianty, kde v případě single-tenantní aplikace dochází ke sdílenému využití některých platformních komponent mezi tenanty (OVS) až po sdílené využití operačního systému v daném virtuálním stroji, budeme dále nazývat „smíšené modely single-tenantní aplikace na IaaS/PaaS). [2] [6]

3. **Single-tenantní aplikace na ICT infrastruktuře zákazníka:** Každý zákazník má vlastní instalaci aplikace ve svém technologickém prostředí (včetně HW-serverů, ať již on-premise nebo na vyhrazených serverech v modelu tradičního outsourcingu). Tato varianta, jak vyplývá z analýzy definice CC výše, nenaplňuje znaky CC v žádné z architektonických vrstev.

3. Vliv zvolené varianty provozu aplikace na zápis do katalogu cloud computingu

Pro zápis řešení aplikačního SW formou služby do katalogu cloud computingu platí:

Model	Požadavky na zápis do katalogu CC
(1) Čistě multi-tenantní model poskytování aplikace formou služby – SaaS	Nabídka **aplikace formou služby**, která plně využívá **multi-tenantní model** (tj. vícenásobné využití jedné instance kódu aplikace v operační paměti pro více tenantů/OVS), **musí** být zapsána v katalogu CC (list „SaaS a smíšené modely“). Využívané služby IaaS/PaaS **musí** být zapsány v katalogu CC.
(2a) Single-tenantní aplikace formou služby provozovaná na IaaS/PaaS, smíšený model	Nabídka **aplikace formou služby**, která využívá **smíšený model**, tj. každému tenantu/OVS je spuštěna **samostatná instance kódu aplikace** v operační paměti, avšak **některé platformní komponenty** jsou využívány **multi-tenantně** (tedy jako PaaS nebo IaaS), **může, avšak nemusí** být zapsána v katalogu CC (v listu „SaaS a smíšené modely“). Viz další podrobnosti pod tabulkou. Využívané služby (komponenty) IaaS/PaaS **musí** být zapsány v katalogu CC.
(2b) Čistě single-tenantní model aplikace formou služby, na cloudové platformě IaaS	**Nabídka aplikace formou služby,** která je postavena na **single-tenantním modelu aplikace** (samostatná instance kódu aplikace pro každého tenanta) **a využívá pouze single-tenantní komponenty** na úrovni platformního SW (jako např. vlastní instanci SQL serveru pro každého tenanta a vlastní instanci Active Directory pro každého tenanta), nicméně využívá cloudových služeb IaaS, **může, avšak nemusí** být zapsána v katalogu CC (list „SaaS a smíšené modely“). Taková aplikace poskytovaná formou služby (subskripce) externím poskytovatelem stále naplňuje definici cloud computingu dle ZoISVS (sdílení zdrojů na úrovni IaaS). Využívané služby IaaS **musí** být zapsány v katalogu CC.
(3) Single-tenantní, on-premise	Aplikace ani infrastrukturní komponenty **nemohou** být zapsány v katalogu CC. Single-tenantní aplikace, instalovaná na vlastní (nesdílené) ICT infrastruktuře zákazníka (on-premise), případně na dedikované (nesdílené) HW infrastruktuře v modelu tradičního outsourcingu nebo v modelu housingu, nebude zapsána v katalogu CC, neboť nenaplňuje definici CC dle ZoISVS v žádné z úrovní IaaS, PaaS nebo SaaS.

- Pro **použité multitenantní platformní komponenty** v případech (2a) a (2b) výše platí, že musí projít zápisem nabídky, a to:
    - buď samostatně ve třídě IaaS/PaaS, a to zejména pokud jde o využití platformní komponenty provozované jiným poskytovatelem, a přeprodávané poskytovatelem aplikace. V případě přeprodeje (i v případě pouhého zahrnutí služeb IaaS/PaaS od jiného materiálního poskytovatele do svojí fakturace) musí být poskytovatel aplikace zapsán i jako přeprodejce těchto platformních služeb IaaS/PaaS;
    - nebo v rámci zápisu nabídky aplikace formou služby materiálního poskytovatele SaaS (nebo smíšeného modelu), kdy je materiální poskytovatel aplikace současně i materiálním poskytovatelem platformy IaaS/PaaS (tedy když platforma IaaS/PaaS je součástí stacku poskytovatele aplikace). V takovém případě musí být tyto komponenty pro účely zápisu nabídky uvedeny jako součást využívané cloudové platformy na certifikátech řady ISO 27000 a případně i SOC2 Type 2 reportu, pokud se jimi dokládá zapisovaná bezpečnostní úroveň.
- **Poskytovatel aplikace v modelech (1), (2a) a (2b)** musí být zapsán v katalogu CC (jedná se minimálně o přeprodej platformy IaaS/PaaS)
- Pouze takové aplikační řešení dodavatele, které nesplňuje podmínku definice cloudové služby, tj. využívá single-tenantní model aplikace nad dedikovanými instancemi platformního a infrastrukturního SW až po dedikovanou instanci hypervizoru a vyhrazené procesory serverů (tedy vlastně klasický outsourcing), **nebude zapsáno** do katalogu CC. Na takové řešení se vůbec nevztahují povinnosti dané Hlavou VI ZoISVS, neboť nenaplňuje definici cloud computingu.

4. Seznam použitých zkratek

CC	Cloud Computing
eGC	eGovernment Cloud
IaaS	Infrastructure as a Service, IT infrastruktura jako služba
ISVS	Informační systém veřejné správy
Materiální poskytovatel	Poskytovatel, který službu cloud computing produkuje. Materiální poskytovatel může mít řady přeprodejců, kteří služby materiálního poskytovatele přeprodávají koncovým zákazníkům.
Multi-tenantní software	Software, jehož jedna instance uložená v operační paměti poskytuje funkcionalitu uživatelům více zákazníků současně.
OVS	Orgán veřejné správy
PaaS	Platform as a Service, IT platforma jako služba
SaaS	Software as a Service, aplikační software jako služba
Single-tenantní software	Software, jehož jedna instance spuštěná v operační paměti poskytuje funkcionalitu uživatelům jednoho zákazníka.
ZoISVS	Zákon č. 365/2000 Sb., o informačních systémech veřejné správy

5. Reference a použité zdroje

[1] Gartner Group: Definition of Software as a Service (SaaS), Gartner Information Technology Glossary: https://www.gartner.com/en/information-technology/glossary/software-as-a-service-saas. Gartner předpokládá „1 to many model“ (all contracted customers), pro common code and data.

[2] Wikipedia: https://en.wikipedia.org/wiki/Software_as_a_service. SaaS je typicky multitenant, ale uvádí se také „but sometimes they offer a siloed environment for an additional fee."

[3] IBM: https://www.ibm.com/topics/saas. Uvádí se v detailu, že „SaaS applications use multi-tenant architecture, in which a single instance of the application serves every customer.“

[4] IBM: https://www.ibm.com/topics/multi-tenant. Uvádí se, že „single instance of a software application (and its underlying database and hardware) serves multiple tenants“

[5] Wikipedia: https://en.wikipedia.org/wiki/Multitenancy. Uvádí vývoj směrem k multi-tenantním aplikacím a popisuje jejich vlastnosti, výhody a nevýhody.

[6] Workos: https://workos.com/blog/singletenant-vs-multitenant. V detailech se zmiňuje „Mixed-tenancy architecture“ a připouští se, že SaaS může mít různé modely, viz část „For SaaS apps, the multi-tenant architecture is almost always the better choice — you can deploy a single instance of your app and serve a huge number of customers, from 1 to 10,000. Adding more features to your app is also easier since you only need to push changes to a single instance. There are however some cases you'll want to go with a single-tenant architecture — when security regulations and data protection laws say so and when you want to support self-hosting.“