27.11.2020

# Postup a hlavné kroky pre vytvorenie projektu vo Vládnom cloude

Informácie potrebné pre vytvorenie projektu vo Vládnom cloude

Martin Balla

# Obsah

# Súhrn

Tento dokument je určený pre organizácie štátnej správy, ktoré majú v pláne využívať služby Vládneho cloudu platformy IaaS, ktorú prevádzkuje Ministerstvo vnútra Slovenskej republiky a ešte na tejto platforme neprevádzkujú žiadny projekt.

V dokumente je popísaná základná terminológia Vládneho cloudu a štruktúra organizácii vo Vládnom cloude. Taktiež sa tu nachádza základný technický popis prostredia, v ktorom si organizácie vytvárajú projekty, a postup pri vytváraní prvého projektu.

# Vymedzenie základných pojmov

- IaaS – Infraštruktúra ako služba (angl. Infrastructure as a Service)
- Vládny cloud – Pre potreby tohto postupu sa pod pojmom Vládny cloud myslí len časť IaaS platformy v prevádzke Ministerstva Vnútra Slovenskej republiky
- Prevádzkovateľ - Ministerstvo Vnútra Slovenskej republiky
- Cloudové služby – Zoznam služieb Vládneho cloudu sa nachádza v dokumente “Katalóg vládnych cloudových služieb”, ktorý sa dá stiahnuť na stránke https://sk.cloud. Z tohto katalógu sa jedná len o služby v bode 1 Vládne cloudové služby – privátna časť – model IaaS. Jedná sa o virtuálne servery, diskový priestor a sieťové služby
- Tenant – Organizácia štátnej správy, ktorá má záujem o využívanie služieb Vládneho cloudu
- Organizácia – Základná reprezentácia tenanta vo Vládnom cloude, ktorá vzniká na základe podpisu zmluvy
- User – Personalizovaný účet osobu z organizácie
- User manager – User s privilégiami vytvárať, upravovať a mazať ostatných userov v organizácii. Prvého user managera vytvára prevádzka Vládneho cloudu
- Gestor – User s privilégiami vytvárať a schvaľovať projekty vo Vládnom cloude za stranu tenanta
- Projekt – Ucelená skupina cloudových služieb, ktoré prevádzkovateľ poskytuje tenantovi za účelom prevádzky IT systému

# Postup pri vytváraní prvého projektu vo Vládnom cloude

1. Oboznámiť sa so základmi high-level infraštruktúrou Vládneho cloudu.
2. Určiť množstvo požadovaných zdrojov projektu vyskladaním virtuálnych serverov zo šablón zverejnených na stránke https://sk.cloud v sekcii “Katalóg služieb - Aktuálne ponúkané šablóny VM”.
3. Určiť ďalšie služby potrebné na prevádzku projektu. Zoznam služieb je zverejnený na stránke https://sk.cloud v sekcii “Katalóg služieb - Časť poskytovateľ - Ministerstvo vnútra SR”. Z tohto katalógu poskytuje Vládny cloud prevádzkovaný Ministrestvom vnútra Slovenskej republiky ale IaaS služby, teda bod 1 z tohto katalógu.
4. Oslovenie prevádzkovateľa Vládneho cloudu na emailovú adresu cloudinfo@minv.sk so žiadosťou o pracovné stretnutie. Pre efektívnosť stretnutia je potrebné dopredu poslať požadované zdroje na Váš projekt, ktoré Vám vyplynú z bodov 2. a 3. tohto postupu. Taktiež odporúčame poslať dopredu zoznam tém a otázok, ktoré chcete riešiť na stretnutí a stručný popis projektu. Na tomto stretnutí sa prevádzkovateľ a tenant dohodnú taktiež na zmluve, ak ešte nebola podpísaná.
5. Ďalší postup je pre každého tenanta individuálny a bude dohodnutý na pracovnom stretnutí. Zahrňuje riešenie technických otázok, optimalizácia projektu pre Vládny cloud, podrobnejšie vysvetlenie informácii o Vládnom cloude zo strany prevádzkovateľa, schválenie alebo zamietnutie projektu zo strany prevádzkovateľa atď.

# High-level popis infraštruktúry Vládneho cloudu

**Projekt** je hlavnou jednotkou pre IT systém umiestnený vo Vládnom cloude. Organizácia môže mať vytvorených viacero projektov. Projekty spolu nemôžu komunikovať po internej sieti Vládneho cloudu a to ani v prípade, že sa nachádzajú v tej istej organizácii. Projekt môže obsahovať rôzne druhy IT systémov od jednoduchých webových stránok až po komplikované systémy.

Každý projekt ma štyri **prostredia**: Produkčné, Vývojové, Predprodukčné a Testovacie. Prostredia v rámci projektu spolu nemôžu komunikovať po interných sieťach Vládneho cloudu.

Každé prostredie má ďalej štyri **vrstvy**: DMZ, V1, V2 a V3. Komunikácia medzi servermi v rámci jednej vrstvy nie je obmedzená a ani sa nedá obmedziť na úrovni infraštruktúry Vládneho cloudu. Pri komunikácii medzi prostrediami sa využíva system whitelistovania komunikácie, tzn. že v základe je všetká komunikácia medzi vrstvami zakázaná a tenant si povoluje len komunikáciu, ktorú potrebuje na prevádzku projektu. Poloviť sa dá komunikácia len medzi vrstvami DMZ <-> V2, V1 <-> V2 a V2 <-> V3.

Vrstva **DMZ** je určená pre komunikáciu projektu do externých sietí.

Vrstva **V1** je určená pre prepojenie projektu s infraštruktúrou organizácie pomocou SSL tunelu.

Vrstva **V2** slúži na prepojenie ostatných vrstiev.

Vrstva **V3** slúži pre virtuálne servery s najcitlivejším obsahom, napr. databázy a zálohy. K serverom v tejto vrstve sa nedá priamo pripojiť zo serverov, na ktoré sa dá pripojiť z externých sietí.

**Topológia** určuje IP rozsah pre vrstvu, tzn. koľko serverov sa môže maximálne nachádzať v danej vrstve. Definuje sa zvlášť pre každú vrstvu v každom prostredí. Topológia je jediný parameter projektu, ktorý sa nedá meniť v priebehu životného cyklu projektu. Ak tenant potrebuje vytvoriť v niektorej vrstve viac virtuálnych serverov ako si na začiatku rezervoval, jediné riešenie je zrušiť celý projekt a vytvoriť ho nanovo.

**Virtuálne servery** si tenant vyberá z poskytovaných kombinácii CPU, RAM a disk. Zoznam všetkých kombinácii je zverejnený na stránke https://sk.cloud v sekcii “Katalóg služieb - Aktuálne ponukané šablóny VM“. Vytvorenie virtuálneho servera mimo týchto kombinácii nie je možná.

Ku každému virtuálnemu serveru sa dajú pripojiť ďalšie **disky**. Zdieľanie jedného disku medzi viacerými virtuálnymi servermi nie je možné. Vládny cloud poskytuje tri druhy diskov:

- Tier1 – najrýchlejšie disky. Ich kapacita je značne obmedzená a žiadosť o ich využívanie je nutné patrične odôvodniť.
- Tier2 – štandardné HHD disky určené na bežnú prevádzku.
- Tier3 – pomalšie disky určené na dáta, ku ktorým nemusí byť rýchly prístup.

Vládny cloud poskytuje podľa Katalógu služieb pripojenie do **externých sietí**: Internet, GOVNET, KTI, KTI2, MVNET. Z kapacitných dôvodov je možné možné každému prostrediu poskytnúť maximálne 2 IP adresy do Internetu. Počet IP adries do ostatných sietí nie je obmedzený.

**Interné firewallové pravidlá** slúžia na definíciu povolenej komunikácie medzi vrstvami prostredia.

**Externé firewallové pravidlá** slúžia na definíciu povolenej komunikácie do externých sietí z vrstvy DMZ.

Vládny cloud poskytuje službu **load balancera**. V prípade, že sa tenant rozhodne túto službu využívať, bude mu vytvorený kontext na F5 zo základnou licenciou. Konfigurácia tohto load balancera je čisto v kompetencii tenanta, ktorý dostane k danému kontextu prihlasovacie údaje.

Zálohovanie projektov vo Vládnom cloude je riešené formou **snapshotov**, tzn. odtlačkom virtuálneho serveru v rátane pripojených diskov v danom čase. Zálohy serverov v rámci projektu môžu prebiehať v rôznych časoch čo znamená, že napr. obnova clastra z takýchto záloh nie je možná. Snapshoty sa vytvárajú každý deň a ich retencia je 4-5 týždňov. Tenant si nemôže určite presnú dobu zálohovania ani zálohy nad rámec automatizovaného procesu.

Vládny cloud **poskytuje nad rámec katálogu služieb** NTP server a WSUS pre aktualizáciu Windows serverov. Komunikácia do externých sietí je taktiež chránená DDoS ochranou.

Vládny cloud **neposkytuje** DNS server, WAF, antivírusovú ochranu tenantských serverov, SIEM kontexty pre projekty ani žiadne ďalšie služby mimo katalógu služieb a vyššie spomínaných NTP a WSUS.