FAQ – technické

Aké sú časti vládneho cloudu ?

Máme dve dátové centra DC Tajov a DC Kopčianska .

Aké IaaS služby sú v aktuálnom katalógu služieb?

Podrobný zoznam aktuálne poskytovaných služieb je možné nájsť v katalógu služieb. Ako príklad IaaS služieb uvádzame: virtualizované serverové platformy x86 (Windows alebo Linux) a RISC (Unix) rôznej veľkosti (S, M, L, XL) v štyroch bezpečnostných zónach (DMZ, prezentačná, aplikačná a databázová) pre štyri dedikované navzájom od seba oddelené cloudové IaaS prostredia (vývojové, testovacie, predprodukčné a produkčné). Ku každému serveru je možné prideliť úložiská dát rôznej kapacity, priepustnosti a rýchlosti odozvy. Pre každé prostredie je potrebné zadefinovať komunikačné požiadavky a prípadné požiadavky na zálohovanie.

Aké sú dostupné verzie opračných systémov v rámci katalógu služieb

Red Hat Enterprice Linux 7.4 (64bit)

Red Hat Enterprice Linux 6.6 (64bit)

CentOS 7-1611 (64 bit)

CentOS 6.7 (64Bit)

Microsoft Windows Server 2012 R2 (64bit)

AIX 7.1 TL3 (64Bit)

Ako je zabezpečené aby iní zákazníci nemohli vidieť/pristupovať k mojím systémom vo vládnom cloude?

Systémové zabezpečenie je na komunikačnej úrovni infraštruktúry. V cloude je pre vaše systémy vytvorené izolované výpočtové prostredie, na ktoré viete pristupovať len pomocou VPN. Nad systémami, ktoré umiestnite do cloudu, máte plnú kontrolu.

Ako sú izolované jednotlivé projekty v cloude?

Pre každý projekt je vytvorený systém izolovaných sietí a výpočtových prostredí. Projekt je sieťovo izolovaný od ostatných projektov a môže mať izolované výpočtové prostredia v rámci projektu (napr.: produkčné, testovacie, vývojové). To znamená, že systémy vytvorené v rámci jedného výpočtového prostredia nevidia systémy v inom výpočtovom prostredí, hoci sú v jednom projekte.

Čo sa stane s dátami po vymazaní projektu?

Ukončenie životnosti projektu prebieha v dvoch fázach. Prvá fáza je zablokovanie projektu. Tento stav nastáva ihneď vtedy, keď zákazník požiada o zrušenie projektu. Projekt nie je dostupný, jeho virtuálne servery sú vypnuté, ale na vymazanie sa čaká počas určenej retenčnej doby. Po uplynutí retenčnej doby sú všetky virtuálne servery a ich disky vymazané. To znamená, že pôvodné dáta nie sú adresovateľné. Na všetky záznamové média je uplatnená disk retention policy, kedy v prípade závady je disk ponechaný vo vlastníctve prevádzkovateľa.

Akú výkonnosť služieb mám očakávať od cloudových služieb?

Výkonnosť služieb je určovaná vlastnosťami virtuálneho servera a vlastnosťami externého virtuálneho disku. Virtuálny server je určený šablónami s trojicami hodnôt (vCPU, vRAM, vHDD), externý virtuálny disk je určený veľkosťou (variabilná, zhora ohraničená hodnota) a rýchlosťou prístupu s označením Tier1, Tier2, Tier3 (zostupne). Virtuálne disky požadovanou kvalitou Tier1 sú umiestnené na SSD diskoch a ich použitie je povolené len v produkčnom výpočtovom prostredí. Všetky šablóny pre virtuálne servery a prístupové rýchlosti jednotlivých „Tier“ úrovní sú popísané v katalógu služieb.

Podporuje prístup viacerých virtuálnych serverov k jednému diskovému priestoru?

OpenStack IaaS technologická platforma v súčasnosti nepodporuje prístup viacerých virtuálnych serverov k jednému blokovému zariadeniu / virtuálnemu disku. V prípade potreby je možné využiť zdieľanie dát prostredníctvom služieb NFS, CIFS, atď.

Aký typ diskového priestoru si mám vybrať?

Virtuálny server je inštalovaný na diskoch Tier2. Externé virtuálne disky je možné vyrobiť na Tier1, Tier2 alebo Tier3 (kvalitatívny popis nájdete v katalógu služieb) s využitím nasledujúcich pravidiel:

- **Tier1** – disky tohto typu je povolené vytvárať len v produkčnom prostredí, využíva sa prístupová rýchlosť SSD diskov
- **Tier2** – bežné disky pre štandardné aplikácie
- **Tier3** – pomalšie disky typické pre použitie so zálohovacími archivačnými aplikáciami

Aká je zabezpečená bezpečnosť systémov umiestnených v cloude?

Cloudové prostredie využíva niekoľkoúrovňovú bezpečnostnú ochranu a analýzu zloženú z produktov (napr. Firewall, IPS, IDS, DDoS, SIEM, NBAD a ďalšie.) viacerých renomovaných vendorov. Systémy umiestnené v cloude musia prechádzať celým bezpečnostným perimetrom na základe projektami definovaných pravidiel.

Ako sú rozdelené kompetencie v oblasti bezpečnosti systémov umiestnených v cloude?

Cloud poskytuje bezpečnú infraštruktúru potrebnú na prevádzku informačných systémov. Bezpečnosť samotných informačných systémov je v kompetencii organizácií využívajúcich cloudové služby.

Môžem si do cloudu umiestniť virtuálny appliance?

Nie, v cloude sú presne definované štandardy a poskytované služby. Používateľ cloudových služieb si musí vybrať z vyhradených operačných systémov, veľkostí serverov a pripojených diskových priestorov.

Môžem do cloudu migrovať celý virtuálny server vrátane operačného systému?

Nie, v cloude sú presne definované štandardy a poskytované služby. Používateľ cloudových služieb si musí vybrať z vyhradených operačných systémov, veľkostí serverov a pripojených diskových priestorov.

Je možné v cloude prevádzkovať systému na báze open-source?

Z katalógu služieb je pre takéto účely možné vybrať operačný systém CentOS.

Aká platforma je využitá na automatizácie systémov?

Platforma pre automatizáciu systémov v cloude sa nazýva orchestračná vrstva. V tomto cloude je použitá orchestračná vrstva na báze OpenStack technológie s podporou virtualizačných vrstiev (hypervízorov) Vmware a PowerVC. OpenStack je iniciatíva s účasťou mnohých renomovaných spoločností pre tvorbu orchestračného prostredia. Viac na http://www.openstack.org.

Ako navrhnúť architektúru informačného systému, taka by bol v súlade s architektúrou vládneho cloudu?

Pri vytváraní projektu umožňuje vládny cloud vytvorenie viacerých vrstiev a prostredí. Vrstvy sú označené DMZ, V1, V2, V3. Hierarchia vrstiev je nasledovná : DMZ/V1 – V2 – V3. Komunikácia je povolená len medzi susediacimi vrstvami. Komunikácia do externých sietí (napr. GOVNET, Internet) je povolená len z vrstvy DMZ.

Servery štandardnej trojvrstvovej aplikácie (WEB/APP/DB), ktorá je dostupná z externej siete je potrebné umiestniť nasledovne :

- DMZ – WEB
- V2 – APP
- V3 – DB

V prípade, že jeden server zabezpečuje viacero funkcií (napr. WEB/APP), umiestňujeme servery nasledovne :

- DMZ – WEB/APP
- V2 – DB

V prípade prepojenia vládneho cloudu s internou sieťou vašej organizácie vytvorením site-to-site VPN tunela je WEB servery poskytujúce služby do internej siete potrebné umiestniť do vrstvy V1.

Prostredia umožňujú separáciu produkčných, testovacích a iných inštancií projektu. Komunikácia medzi prostrediami nie je možná. Vládny cloud umožňuje vytvorenie 4 prostredí. V rámci vrstvy prostredia zdieľajú jeden IP rozsah.

Kto je zodpovedný za aktualizáciu operačných systémov?

Vládny cloud poskytuje iniciálne templaty vybraných operačných systémov a infraštruktúru potrebnú na ich aktualizácie. Momentálne sú k dispozícii Microsoft aktualizácie týchto klasifikácií: Critical Updates, Definition Updates, Drivers, Feature Packs, Security Updates, Service Packs, Tools, Update Rollups, Updates.

Sú poskytované pre tieto produkty: Windows Server 2012, Windows Server 2012r2, Office 2013 family, MS SQL Server 2012 (možnosť vyšpecifikovať ďalšie produkty)

Jazyková podpora English (možnosť vyšpecifikovať ďalšie).

Za aktualizáciu prevádzkovaných virtuálnych serverov je zodpovedný používateľ IaaS služieb.

Ktoré podporné služby poskytuje vládny cloud?

Okrem zabezpečenia aktualizácií poskytuje vládny cloud napríklad synchronizáciu času prostredníctvom protokolu NTP. Ďalšie služby sa postupne vo vládnom cloude zavádzajú. Zoznam dostupných služieb je uvedený v aktuálnej verzii katalógu služieb.

Čo ak potrebujem využívať podporné služby, ktoré vládny cloud neposkytuje?

Používateľ cloudových služieb môže takéto podporné služby implementovať v existujúcom IaaS prostredí cloudu alebo ich sprístupniť z externého prostredia.

Do ktorých externých sietí je pripojený vládny cloud?

V súčasnosti je vládny cloud pripojený do externých sietí GovNet, Internet , MVNet – DC Tajov, DC Kopčianska – obsahuje aj pripojenie KTI . Prostredie vládneho cloud je technologicky pripravené na pripojenie do ďalších sietí, pričom ich pripojenie je závislé od požiadaviek konkrétnych systémov a možnosti na strane subjektov prevádzkujúcich externé siete.

Má používateľ cloudu administrátorské privilégiá k jednotlivým virtuálnym serverom?

Áno.

Je vo vládnom cloude implementovaný monitoring služieb?

Monitoring služieb IaaS vo vládnom cloude je implementovaný v zákazníckom rozhraní CSP formou nasledujúcich prevádzkových parametrov:

- virtual server status (hodnota bude reprezentovaná ikonou, VM beží alebo nebeží)
- uptime (časová hodnota definujúca dĺžku behu virtuálneho servera od posledného štartu)
- grafické znázornenie utilizácie parametrov virtuálneho servera RAM, CPU, HDD

Vládny cloud disponuje taktiež s enterprise monitoring systémom zabezpečujúcim monitoring kompletnej IKT infraštruktúry na úroveň jednotlivých komponentov.

Poskytuje vládny cloud službu zálohovania?

Áno, v súčasnosti vládny cloud umožňuje v rámci IaaS služieb zálohovanie snímkov (snapshotov) virtuálnych serverov so všetkými jeho diskami, ktoré sú v pravidelných intervaloch ukladané na TIER III diskoch a následne na páskových médiách. Odporúčanie pre používateľov IaaS služieb je využiť existujúce snímkovanie virtuálnych serverov s vlastným postupom zálohovania súborového systému prípadne databáz a podobne. V budúcnosti sa uvažuje so zriadením centralizovanej služby zálohovania na báze SaaS.