

HYBRIDNÁ IT INFRAŠTRUKTÚRA

Igor HALÁMA

Anotácia

Nástup virtualizácie spôsobil pred niekoľkými rokmi revolúciu v IT tým, že poskytol možnosť oveľa lepšieho využívania hardvérových prostriedkov, rýchlejšieho vytvárania a rušenia serverov, zvýšenú flexibilitu a nové možnosti pri zabezpečení dostupnosti.

Kľúčové slová

virtualizácia, cloud, Microsoft Azure, dátové centrum

Dnes sme svedkami rovnako významnej transformácie, ktorú predstavujú možnosti hybridnej infraštruktúry. Vďaka hybridnému cloudu je možné poskytovať aplikácie s oveľa väčšou flexibilitou a nižšími nákladmi. Rýchlejšie tempo inovácií, umožnené vďaka cloudu, prispieva k zvýšeniu konkurencieschopnosti.

Hlavné výhody cloudu:

- flexibilita – platíte len za to, čo spotrebujete;
- možnosť rýchlej zmeny (škálovania) alokovaných CPU, RAM, úložiska podľa okamžitej potreby;
- veľmi rýchle vytvorenie celej potrebnej infraštruktúry;
- otvorenosť – v cloudu je možné prevádzkovať OS a aplikácie od rôznych dodávateľov;
- bezpečnosť – cloudové dátové centrá sú zabezpečené na takej úrovni, aká je veľmi ťažko dosiahnuteľná pri dátových centrách menšej mierky. Platí to pre všetky aspekty bezpečnosti (fyzickú, infraštruktúrnú, sieťovú, aplikačnú);
- zrýchlenie tempa inovácií – rýchle uvedenie nových aplikácií bez potreby obstarávania potrebného hardvéru;
- presunutie nákladov z investičných (CapEx) na prevádzkové (OpEx);
- okamžitý prístup k najmodernejším službám s vysokou pridanou hodnotou (Machine Learning, Cognitive services, BIG DATA, IoT, ...) bez potreby vstupných investícií.

Riešenia v rámci hybridnej infraštruktúry

Rozšírenie/prepojenie vnútornej infraštruktúry s Cloudom

Cloudové riešenia majú nesporné výhody pre mnohé scenáre, napr. aplikácie a webové stránky s veľkými výkyvmi v požiadavkách na výkon, testovacie a vývojové prostredie a infraštruktúra pre startupy. Na druhej strane, uzavreté riešenie vo vlastnom dátovom centre môže poskytnúť splnenie najprísnejších požiadaviek na bezpečnosť pre aplikácie s kritickými podnikovými dátami. Pokračovanie v prevádzke existujúceho vo vlastnom dátovom centre riešenia má opodstatnenie aj vtedy, keď by migrácia na platformu kompatibilnú s cloudom bola príliš nákladná.

Hybridné scenáre umožňujú na základe analýzy aktuálneho stavu a požiadaviek zákazníka navrhnúť najvýhodnejšie riešenie pre každú z aplikácií. Verejný a privátny cloud a dedikované servery sú prepojené do jednej spolupracujúcej infraštruktúry.

Toto spojenie ponúka kombinované benefity – flexibilitu, škálovateľnosť a zníženie TCO tam, kde je to možné, a splnenie najprísnejších vnútrofirmych predpisov tam, kde je to potrebné.

<https://spu.fem.uniag.sk/fem/sem-eunis/eunis20/>

Business Continuity Management (exe SafeSpace Backup / Site Recovery)

exe SafeSpace Backup a Site Recovery predstavujú službu Disaster Recovery as a Service s využitím prostriedkov cloudu Microsoft Azure. Umožňujú spoľahlivú ochranu serverov s Windowsom aj Linuxom, ktoré môžu byť prevádzkované v prostredí VMWare, Hyper-V alebo na fyzickom železe. Okrem zálohovania je možné v prostredí cloudu Microsoft Azure vytvoriť s minimálnymi počiatočnými nákladmi vzdialené záložné dátové centrum, ktoré bude kedykoľvek k dispozícii pre prípad výpadku. Nekonečné výpočtové zdroje Azure je tiež možné využiť na testovanie obnovy. SafeSpace Backup je tiež možné využiť na dlhodobú archiváciu údajov na 99+ rokov.

Manažment a monitoring hybridnej infraštruktúry

Poskytujeme nástroje pre komplexný monitoring a manažment infraštruktúry, fyzickej aj virtuálnej, vo vlastnom dátovom centre aj v hybridnom cloude.

Vzrast verejných, hostovaných a hybridných cloudových riešení prináša nové výzvy pre manažment IT infraštruktúry. Manažment IT infraštruktúry je čoraz menej o tom, čo sa deje za vašim firewallom a čoraz viac o manažmente dát a aplikácií, kdekoľvek sa nachádzajú.

Nástroje pre manažment a monitoring pokrývajú všetky dôležité aspekty manažmentu infraštruktúry a DevOps pre provisioning, konfiguráciu, monitoring, automatizáciu a service management, a to pre akúkoľvek platformu — či už vo vlastnom dátovom centre, Azure a Amazon Web Services (AWS) cloud s operačnými systémami Windows Server, Linux, VMware alebo OpenStack.

Azure Information Protection

Microsoft Azure Information Protection umožňuje klasifikáciu a označovanie informácií v čase ich vytvárania. Na citlivé údaje je možné aplikovať ochranu informácií, ktorá spočíva v šifrovaní, overovaní používateľov a pridelení oprávnení na základe identity. Klasifikácia môže byť plne automatická, ovládaná používateľom alebo nastavená na základe odporúčaní. Keď sú údaje klasifikované a označené, je možné aplikovať ochranu na základe klasifikácie. Klasifikácia a ochrana sú perzistentné, cestujú s údajmi, takže dokumenty sú identifikovateľné a chránené po celý čas – bez ohľadu na to, kde sú uložené a s kým sú zdieľané. Používateľské rozhranie je jednoduché a intuitívne, takže nijako neovplyvní prácu s dokumentami. Máte taktiež k dispozícii dokonalý prehľad a kontrolu nad zdieľanými dokumentami. Azure Information Protection umožňuje ochranu osobných údajov podľa požiadaviek GDPR.

Dev/Test scenáre

DevTest Labs v Microsoft Azure je služba, ktorá poskytuje vývojárom a testerom prostredie, v ktorom si samoobslužným spôsobom môžu rýchlo vytvoriť a potom manažovať potrebnú infraštruktúru za súčasného šetrenia prostriedkov. Opakované vytváranie Windows a Linux infraštruktúry je urýchlené prostredníctvom šablón. Náklady je možné mať efektívne pod kontrolou – dajú sa nastaviť finančné limity, ako aj obmedziť to, aké výkonné a teda drahé VM si konkrétny vývojár môže postaviť.

Kontakt

Igor Haľama, Presales Technology Consultant

exe, a.s., Slávičie údolie 6, 811 02 Bratislava | T: +4212 6729 6791 M: +421 907 446 128

Recenzent: Ing. Jozef Koricina, Trnavská univerzita v Trnave