Všeobecné podmienky pre pripojenie do verejnej časti vládneho cloudu

Microsoft Azure

Popis riešenia verejnej časti vládneho cloudu v Microsoft Azure

Riešenie reprezentuje cloudovú infraštruktúru od spoločnosti Microsoft Azure (ďalej len „infraštruktúra **Azure**“ alebo „**Azure**“), ktorá zabezpečuje poskytovanie a dostupnosť cloudových služieb. Tieto služby sú zaradené do katalógu vládnych cloudových služieb vedeného Ministerstvom investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (ďalej len „**MIRRI SR**“), ako súčasť verejnej časti vládneho cloudu.

V kontexte manažmentu vládnych cloudových služieb sa v cloudových riešeniach implementovaných do verejnej časti vládneho cloudu uplatňuje koncept „Single Tenant“. Single tenant koncept v kontexte znamená, že organizácia MIRRI SR používa cloudové služby s konceptom jediného nájomcu. Tento koncept zahŕňa "Root Tenant", čo je centrálne prostredie, kde každý odberateľ cloudových služieb má prístup k presne ohraničenému virtuálnemu priestoru pre každý projekt. Projektom sa rozumie projekt v zmysle vyhlášky o riadení projektov alebo informačná technológia, ktorá nespĺňa formálne požiadavky projektu podľa vyhlášky o riadení projektov a bude umiestnená v cloudovej infraštruktúre Microsoft Azure.

Prístup do tohto virtuálneho priestoru je riadený prostredníctvom definovaných prístupových rolí odberateľa, čím sa zabezpečuje, že každý používateľ má prístup len k relevantným zdrojom a funkciám projektu, v rámci jedného tenanta.

Správcom tohto virtuálneho priestoru je MIRRI SR, ktoré má oprávnenia na monitorovanie fakturácie, výkonnosti a súladu s politikami pripojenia do infraštruktúry Azure (ďalej len „politiky Azure“). Tieto práva sú navrhnuté tak, aby zabezpečili bezpečnosť, dôvernosť a integritu údajov bez akéhokoľvek získavania metaúdajov zo zdrojov projektu.

V rámci konceptu single tenant sa využíva dizajn "hub & spoke" topológie sietí. Spomínaná topológia predstavuje architektonický model dedikovaných virtuálnych sietí, ktorých súčasťou je centrálne umiestnený "hub" spojený s viacerými takzvanými "spoke". Centrálny hub v topológii slúži aj ako miesto, kde sú umiestnené kritické bezpečnostné prvky, ako je firewall a ďalšie centrálne zariadenia na monitorovanie a riadenie bezpečnosti. Implementovaním dizajnu “hub & spoke“ sa zabezpečuje centralizovaná kontrola nad prístupom z verejnej internetovej siete do infraštruktúry Azure (Inbound traffic) a do verejnej internetovej siete z infraštruktúry Azure (outbound), z internetu a von do internetu, detekciou hrozieb a zabezpečením dát v rámci celej infraštruktúry Azure (vrátane virtuálneho priestoru odberateľa). Jednotlivé projekty, reprezentované "spoke", môžu byť spravované a monitorované individuálne tzn. v správe odberateľa pričom pravidlá oddelenia a izolácie od iných projektov ostávajú zachované.

Takýto dizajn umožňuje efektívne riadenie a monitorovanie komunikácie medzi jednotlivými časťami infraštruktúry Azure. Zároveň poskytuje flexibilitu a škálovateľnosť, pretože nové projekty môžu byť ľahko pridané alebo odstránené bez výrazných zásahov do celkovej centrálnej infraštruktúry. Celkový bezpečnostný rámec je zoskupený a riadený centrálnym hubom, čo zabezpečuje konzistentnú a efektívnu implementáciu bezpečnostných opatrení.

Odberateľ, ktorý zvažuje umiestnenie svojich služieb vo verejnej časti vládneho cloudu, je povinný oboznámiť sa s technickým riešením a pravidlami vyplývajúcimi z tohto riešenia definovanými v tomto dokumente.

Požiadavky na bezpečnosť prístupov identít

Pre prístup do prostredia je nevyhnutné poskytnúť informácie o identitách, ktoré majú byť prizvané v podobe rolí do vládneho cloudu v infraštruktúre Azure. Vo verejnej časti vládneho cloudu sú identity odberateľa prizývané ako hosťovské účty, čo platí aj pre externých dodávateľov projektu. MIRRI SR má na starosti správu Microsoft Entra ID v rozsahu prizývania identít, vytvárania a pridelenia oprávnení do

bezpečnostných skupín. Následne je potrebné mať zriadený autentifikátor na overenie identity pomocou multifaktorovej autentifikácie (ďalej len „MFA“).

Aplikáciu MFA je môžné inštalovať prostredníctvom tohto odkazu:

Download and Install the Microsoft Authenticator App

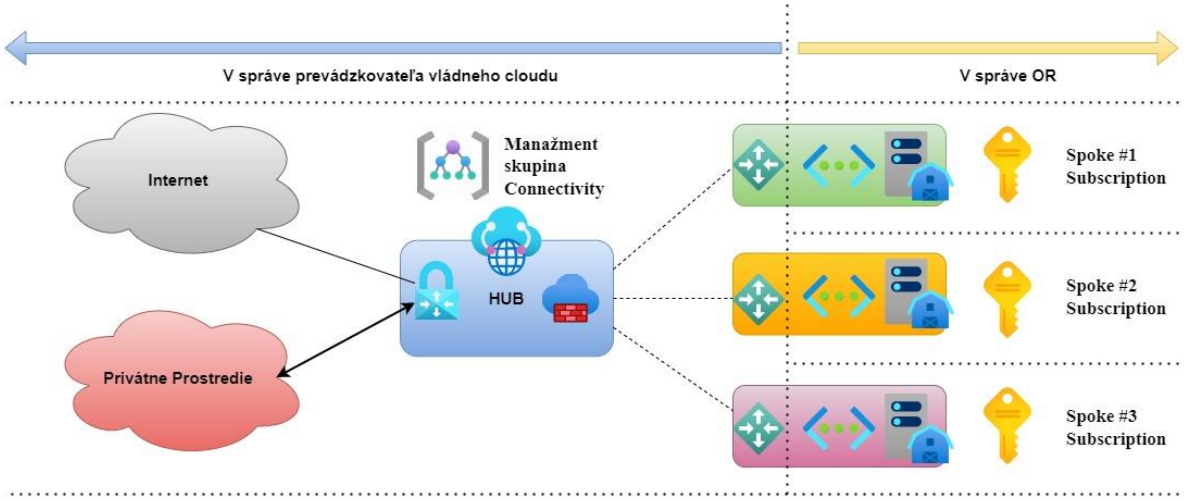
Technické požiadavky

Technické požiadavky predstavujú súbor špecifikácií a kritérií, ktoré musia byť splnené pre úspešnú implementáciu a prevádzku technologických systémov, aplikácií alebo projektov. Tieto požiadavky definujú minimálne štandardy a parametre, ktoré zabezpečujú správnu funkčnosť, bezpečnosť a efektívnosť technických riešení.

Hub and Spoke Topológia je implementovaná s nasledujúcimi charakteristikami:

- Hub predstavuje centrálny bod, manažovanú cloudovú službu Virtual WAN, kde sú lokalizované všetky zdieľané služby, vrátane prvkov ako Firewall, AppGW, VPN spojenia a Spoke spojenia (tzv. peering službou).
- Spokes predstavujú dedikované virtuálne siete pre konkrétny projekt s definovaným IP rozsahom, ktorý sa môže ďalej rozdeliť na viaceré prefixy (subnet). Spoke predstavuje izolovanú časť infraštruktúry, ktorá je spojená s centrálnym hubom pomocou peering služby.

Čo je virtuálny WAN



Obrázok 1: Diagram verejnej časti vládneho cloudu v Azure.

Subscription predstavuje predplatné a organizáciu zdrojov:

- Poskytuje prístup k rôznym cloudovým službám infraštruktúry Azure, ako sú virtuálne siete, stroje, úložiská dát, databázové riešenia a ďalšie.
- Poskytuje nástroje na správu a monitorovanie cloudových prostredí v infraštruktúre Azure pre efektívne využívanie zdrojov.
- Riadenie prístupu a bezpečnosti, poskytuje mechanizmus na riadenie prístupu, čo umožňuje definovať špecifické oprávnenia pre jednotlivé skupiny zdrojov.
- Štruktúrovaná správa umožňuje štruktúrovanú a efektívnu správu zdrojov, ktoré patria k rôznym projektom, tímom alebo organizačným útvarom organizácie.
- Izolácia zdrojov od ostatných, čím sa minimalizuje riziko neoprávnenej manipulácie alebo prístupu.

Virtual Cloud Network (ďalej len „**Vnet**“) a ich použitie:

- Poskytuje sieťové oddelenie jednotlivých projektov využívaním cloudovéj služby Vnet. Prevádzkovateľ verejnej časti vládneho cloudu prideľuje rozsah IP adries pre každý jeden nový projekt, ktorý je implementovaný v cloude bez nadväznosti na predchádzajúce on premise reišenie (Green Field projekt). Táto konfigurácia zabezpečuje efektívne oddelenie sieťových zdrojov pre každý projekt.

Poznámka: Ak sa jedná o projekt, ktorý má nadväznosť na on-premise riešenie je potrebná konzultácia o pridelení IP rozsahov.

Naming Convention a Tagging (Menná konvencia a značkovanie) charakteristika:

- Súbor pravidiel a štandardov, ktoré určujú spôsob pomenovávania a identifikácie cloudových zdrojov a objektov infraštruktúry Azure , medzi ktoré patria virtuálne stroje, úložiská, siete, alebo iné komponenty.
- Cieľom menných konvencií a značkovaní je zabezpečiť jednotný a systematický prístup k identifikácii zdrojov v celom virtuálnom prostredí, čo prispieva k efektívnemu riadeniu, organizácii a sledovaniu zdrojov v Azure.
- Menná konvencia pre cloudové služby poskytované v rámci infraštruktúry Azure je dostupná na GitHube.

Menná Konvencia pre Microsoft Azure

Konvencia pomenovania Taggov

Poznámka: Ak sa jedna o cloudové služby, ktoré nie sú v mennej konvencii uvedené, je potrebné skutočnosť nahlásiť na cloud kanceláriu MIRRI na adrese cloud@mirri.gov.sk

Technické pravidlá využívania vládnych cloudových služieb infraštruktúry Azure vo verejnej časti vládneho cloudu požadujú, okrem vyššie uvedeného, aj implementáciu nasledovných princípov :

- Používanie zdieľaných komponentov dedikovaných pre bezpečnosť akým je centrálny hub.
- Efektívne využívanie služieb v cloude tak, aby sa pre každý projekt nemuseli alokovať nové dedikované zdroje, ktoré nebudú dostatočne využívané.

Medzi najčastejšie používané zdieľané komponenty v infraštruktúre Azure patria:

Azure Firewall

Bastion

AppGW

VPN-S2S/P2S/ExpressRoute

Private DNS Zones

DNS Private Endpoints

Požiadavky pre finančné riadenie predstavujú pravidlá využívania zdrojov a tomu zodpovedajúcich výdavkov v infraštruktúre Azure

Kvóta je obmedzenie s nasledujúcimi charakteristikami:

- Určuje množstvo zdrojov, ktoré môže daný projekt v infraštruktúre Azure využívať. To zahŕňa virtuálne stroje, úložný priestor, sieťové komponenty a ďalšie.
- Cieľom je optimalizovať využitie zdrojov a pridelenie dostupných zdrojov na základe vyplnených žiadostí.

Budget predstavuje službu s nasledujúcimi charakteristikami:

- Slúži na sledovanie a riadenie výdavkov v rámci infraštruktúry Azure, čím umožňuje efektívne hospodárenie s finančnými prostriedkami.
- Pomáha predchádzať neplánovaným nákladom a zabezpečuje, že projekt operuje v rámci stanovených finančných limitov.
- Poskytuje nástroje na monitorovanie a správu nákladov na služby využívané v infraštruktúre Azure, vrátane sledovania aktuálneho stavu výdavkov v porovnaní s definovaným rozpočtom.

Organizačné pravidlá, ktorých používanie je nevyhnutné na zabezpečenie správnej funkčnosti informačnej technológie pri využívaní infraštruktúry Azure:

Povinnosti projektu pri používaní IaaS služieb

- **Aktualizácia operačného systému a softvéru**: Zabezpečiť, aby bol operačný systém a inštalovaný softvér vždy v aktuálnej verzii. V prípade použitia nepodporovanej alebo nelicencovanej služby, pričom poskytovateľ cloudových služieb nenesie zodpovednosť za ich výpadok a správu.
- **Sledovanie bezpečnostných noviniek**: Pravidelne monitorovať novinky v oblasti bezpečnosti týkajúce sa používaného operačného systému a softvéru.
- **Reakcia na bezpečnostné audity**: Okamžite reagovať na výsledky bezpečnostných auditov, pričom časový rámec reakcie by mal byť dostatočne krátky na zachovanie bezpečnosti poskytovanej služby.
- **Dodržiavať konvencie**: Povinnosť dodržiavať mennú a značkovaciu konvenciu ("naming convention" a „tagging“) pri pomenovávaní a identifikovaní cloudových zdrojov.
- **Povinnosť dodržiavať stanovený rozsah cloudových služieb**: Dodržiavať stanovený rozsah poskytovaných cloudových služieb a nevyužívať zdroje mimo tejto definície.

Povinnosti projektu pri používaní PaaS/SaaS služieb

- **Dodržiavať odporúčanie poskytovateľa cloudových služieb**: Riadiť sa odporúčaniami poskytovateľa cloudových služieb, ktoré sú verejne dostupné na oficiálnych stránkach poskytovateľa.
- **Používať odporúčanú verziu manažovanej cloud služby:** Vybrať a používať odporúčanú verziu manažovanej cloudovéj služby tak, aby boli dodržané stanovené termíny End-of-Support (EoS) a End-of-Life (EoL) od poskytovateľa. V prípade spravovania služby v nepodporovanej verzii môže byť služba vypnutá alebo poskytovaná bez podpory poskytovateľa, pričom poskytovateľ cloudových služieb nenesie zodpovednosť za ich výpadok a správu.
- **Dodržiavať konvencie**: Povinnosť dodržiavať mennú a značkovaciu konvenciu ("naming convention" a „tagging“) pri pomenovávaní a identifikovaní cloudových zdrojov.
- **Povinnosť dodržiavať stanovený rozsah cloudových služieb:** Dodržiavať stanovený rozsah poskytovaných cloudových služieb a nevyužívať zdroje mimo tejto definície.

Pravidlá pre audit virtuálneho prostredia a používaných cloudových služieb v Azure

Audit procesu a nastavení

- Sledovanie a hodnotenie celkového virtuálneho prostredia v Azure sú usmerňované s cieľom zabezpečiť dodržiavanie štandardov, ktoré zahŕňajú ISO normy, ako aj najlepšie postupy poskytovateľa cloud služieb, a to v súlade s politikami na zabezpečenie pravidiel informačnej bezpečnosti.
- Azure politiky je mechanizmus, ktorý umožňuje definovať, implementovať a spravovať pravidlá pre správu zdrojov v cloude s cieľom dosiahnuť zhodu s MIRRI SR bezpečnostnými štandardmi.
- Nezávislý audit a kontrola nastavení predstavuje overenie, nastavenia všetkých aspektov virtuálneho prostredia, s dôrazom na bezpečnosť a v súlade s predpísanými politikami MIRRI SR. Analýza konfigurácie vychádzajúca z auditov procesu a nastavení vykonávaná ad-hoc.

Reakcie na zistenia auditu

- **Promptné reakcie na identifikované bezpečnostné nedostatky**: promptné a adekvátne reakcie na identifikované bezpečnostné nedostatky alebo nesúlad s najlepšími postupmi.
- **Zabezpečenie ssl/tls používania**: ak audit odhalí používanie nezabezpečeného prenosu dát (napr. http namiesto https), od projektu sa očakáva včasné a riadne riešenie tohto nedostatku alebo jeho odôvodnenie .
- **Vyhodnotenie bezpečnostných praktík:** sledovanie dodržiavania bezpečnostných pravidiel a odporúčaní, s výzvami na ich aktualizáciu a prípadné zlepšenia.

Pravidlá pre implementáciu a migráciu informačných technológií do infraštruktúry Azure predstavujú základné princípy prechodu projektov, technológií, aplikácii do infraštruktúry vládnych cloudových služieb

Plánovanie nového projektu

- **Administratívne požiadavky**: Splnenie administratívnych požiadaviek, ako je kategorizácia, Sizing, a žiadosť o poskytnutie cloudových služieb.
- **Povinnosť prispôsobenia technológie**: Odberateľ, ktorý plánuje nový projekt, je zaviazaný optimalizovať informačnú technológiu pre "cloud native" požiadavky s výrazným dôrazom na minimalizáciu používania IaaS služieb.
- **Odôvodnenie pri použití IaaS**: V prípade požiadavky na IaaS služby musí odberateľ písomne zdôvodniť skutkový stav použitia IaaS, pričom tento je povolený za predpokladu, že neexistuje rovnocenná alternatíva pre vybranú IaaS službu alebo koncový IT produkt nie je kompatibilný s PaaS alebo SaaS cloudovú službou.
- Povinnosť využiť PaaS a SaaS cloudových služieb, ak je to z povahy projektu možné.

Migrácia existujúceho projektu

- **Hodnotenie AS IS prostredia**: Odberateľ, ktorý zvažuje migráciu existujúceho projektu, je povinný vypracovať komplexné hodnotenie súčasného prostredia. Tento proces vyžaduje dôkladné spracovanie všetkých potrebných dokumentov, ako sú Sizing a kategorizácia, TCO.
- **Návrh nahradenia služieb**: Výstupom hodnotenia musí byť konkrétny návrh nahradenia existujúcich IaaS služieb ekvivalentnými alebo obdobnými PaaS alebo SaaS službami, s dôrazom na dosiahnutie ekonomickej efektívnosti.
- **Zoznam plánovaných služieb**: Odberateľ je povinný predložiť konečný zoznam plánovaných služieb, spolu s počtami a s indikáciou maximálneho odhadovaného počtu služieb.
- **Odôvodnenie pri použití IaaS**: V prípade požiadavky na IaaS služby musí odberateľ písomne zdôvodniť skutkový stav použitia IaaS, pričom tento je povolený za predpokladu, že neexistuje rovnocenná alternatíva pre vybranú IaaS službu alebo koncový IT produkt nie je kompatibilný s PaaS alebo SaaS cloudovú službou.

Stanovenie časového aspektu migrácie: Povolená časová alokácia pre migráciu je maximálne obdobie 3 kalendárnych mesiacov, v odôvodnených prípadoch môže MIRRI SR povoliť predĺženie doby migrácie na ďalšie 3 kalendárne mesiace.