MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Všeobecné podmienky pre pripojenie do verejnej časti vládneho cloudu

Microsoft Azure

v:2.0

Popis riešenia verejnej časti vládneho cloudu v Microsoft Azure

Riešenie predstavuje cloudovú infraštruktúru od spoločnosti Microsoft Azure (ďalej len „infraštruktúra Azure“ alebo „Azure“), ktorá zabezpečuje poskytovanie a dostupnosť cloudových služieb. Tieto služby sú zahrnuté v katalógu vládnych cloudových služieb, ktorý spravuje Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (MIRRI SR) ako súčasť verejnej časti vládneho cloudu.

V manažmente vládnych cloudových služieb sa v rámci riešení implementovaných vo verejnej časti cloudu využíva koncept Single Tenant, čo znamená, že MIRRI SR používa cloudové služby s jediným tenantom. V tomto koncepte "Root Tenant" predstavuje centrálne prostredie, kde každý odberateľ cloudových služieb má prístup do presne ohraničeného virtuálneho priestoru pre konkrétny projekt. Prístupy do tohto priestoru sú riadené prostredníctvom rolí, ktoré definujú prístup k zdrojom a funkciám v rámci daného tenanta.

Prístupové práva v Azure

Globálny administrátor v Azure

Globálny administrátor má najvyššie práva v Microsoft Azure a zodpovedá za komplexnú správu a konfiguráciu cloudového prostredia.

Hlavné úlohy a práva:

- **Správa užívateľov a skupín**: Vytváranie a úprava užívateľských účtov a skupín v Azure Active Directory.
- **Konfigurácia predplatného a zdrojov**: Úplná kontrola nad všetkými predplatnými a zdrojmi, ako sú virtuálne stroje, úložiská, a siete.
- **Bezpečnostné politiky**: Nastavovanie a úprava bezpečnostných a prístupových pravidiel.
- **Monitorovanie a reporting**: Prístup k nástrojom na monitorovanie výkonu a generovanie reportov.
- **Fakturácia**: Správa fakturačných informácií a nastavení.

Oddelenie správy biznis, aplikačnej a technologickej architektúry MIRRI SR s oprávnením má monitorovať fakturáciu, výkonnosť a súlad s politikami Azure na zabezpečenie bezpečnosti a integrity ochrany údajov. Tieto oprávnenia sú obmedzené na monitorovanie a neumožňujú priamy prístup k údajom projektu.

Poznámka: Globálny administrátor, je osoba zodpovedná za riadenie sekcie ITVS, má nevyhnutný prístup k celému prostrediu len v prípade narušenia bezpečnosti, kde je potrebné zabezpečiť rýchlu

reakciu a riešenie problému.

Ostatné role a oprávnenia v Azure (RBAC)

V prostredí Microsoft Azure je k dispozícii niekoľko rolí, ktoré určujú úroveň prístupu a možností správy. Tieto roly sa priraďujú k jednotlivým používateľom alebo skupinám, aby sa zabezpečil princíp minimálnych oprávnení (least privilege).

Popis skupín a oprávnení o ktoré je možné požiadať:

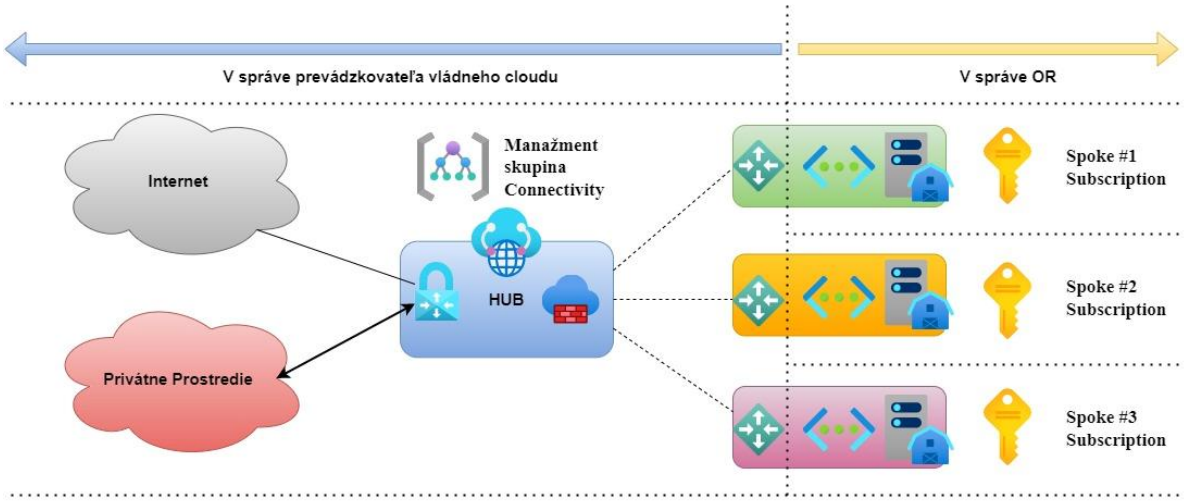
https://mirri.gov.sk/wp-content/uploads/2024/01/Azure_RBAC_Roles_Template-.xlsx

---

Každý odberateľ, ktorý plánuje umiestniť svoje služby vo verejnej časti vládneho cloudu, je povinný oboznámiť sa s technickým riešením a pravidlami vyplývajúcimi z tohto dokumentu, aby zabezpečil správne fungovanie a bezpečnosť svojho projektu v rámci tejto infraštruktúry.

Architektúra je postavená na topológii Hub & Spoke s centralizovaným riadením pripojení a bezpečnosti. Táto architektúra je rozdelená do dvoch častí – časť v správe prevádzkovateľa verejnej časti vládneho cloudu a časť v správe orgánom riadenia (OR), ktoré využívajú verejnú časť vládneho cloud-u.

Architektúra zabezpečuje efektívne riadenie cloudových zdrojov a sietí s vysokou úrovňou bezpečnosti a izolácie medzi jednotlivými projektmi. Hub & Spoke model umožňuje centralizovanú kontrolu nad prístupmi a bezpečnostnými prvkami v cloude, pričom jednotlivé organizácie majú možnosť samostatne spravovať svoje projekty a zdroje v rámci pridelených Subscription.



Obrázok 1 HA Diagram verejnej časti vládneho cloudu Azure

1. Hub:

Hub predstavuje centrálny bod infraštruktúry, ktorý spravuje konektivitu medzi externými zdrojmi a privátnym prostredím prostredníctvom manažovanej služby Virtual WAN. Je zodpovedný za bezpečnosť a správu prístupov. Je prepojený s verejným internetom a privátnym prostredím prostredníctvom Firewallu, VPN a APPGW, čo zabezpečuje kontrolovaný prístup k zdrojom v sieti. Manažment skupina Connectivity zodpovedá za riadenie sieťovej komunikácie v celom Hub prostredí v správe cloud kancelárie MIRRI SR.

2. Spoke:

Každý Spoke predstavuje oddelené virtuálne prostredie pre konkrétny projekt alebo organizačnú jednotku. Tieto Spoke sú prepojené na centrálny hub prostredníctvom bezpečnostných pravidiel a sieťových pripojení. Každý Spoke má pridelenú svoju vlastnú Subscription, čo umožňuje jednotlivým projektom alebo organizačným útvarom riadiť si svoje vlastné cloudové zdroje.

3. Virtuálne siete:

Vnet poskytuje sieťové oddelenie jednotlivých projektov využívaním cloudovéj služby Vnet. Prevádzkovateľ verejnej časti vládneho cloudu prideľuje rozsah IP adries pre každý nový projekt implementovaný v cloude bez nadväznosti na predchádzajúce on-premise riešenie (Green Field projekt). Ak je projekt migrovaný (Brown Field projekt) a nadväzuje na on-premise riešenie alebo si vyžaduje rozsiahlu úpravu komponentov prostredia, je potrebné konzultovať pridelenie IP rozsahov s MIRRI SR. (*V prípade, že sa pridelený rozsah od prevádzkovateľa dostane do duplicity s on-premise systémom, je potrebné zriadiť nový HUB, ktorému bude následne priradený IP rozsah z on-premise prostredia*).

4. Subscription:

Každý Spoke má svoju vlastnú Subscription, ktorá je spravovaná danou OR. Subscription slúži ako kontajner na správu zdrojov, vrátane virtuálnych sietí, výpočtovej kapacity a úložiska. Každá Subscription je izolovaná, čo zaručuje nezávislosť a bezpečnosť medzi jednotlivými Spoke.

5. Manažment Connectivity:

Manažment skupina Connectivity zodpovedá za riadenie sieťovej infraštruktúry, vrátane pripojení medzi Hub, Spoke a vonkajšími sieťami. Táto úroveň manažmentu zabezpečuje správu prístupov, kontrolu komunikácie a integráciu bezpečnostných prvkov v rámci celej topológie v správe cloudovéj kancelárie MIRRI SR.

6. Externé a privátne pripojenia:

Architektúra podporuje prístup z internetu a z privátnych prostredí (napr. z interných sietí organizácií), pričom komunikácia je riadená centralizovaným hubom. Firewall slúži na zabezpečenie inbound a outbound prenosov dát medzi cloudovou infraštruktúrou a vonkajšími sieťami.

Požiadavky na bezpečnosť prístupov identít

Pre prístup do prostredia je potrebné poskytnúť informácie o identitách, ktoré majú byť prizvané do vládneho cloudu Azure, s pridelením príslušných rolí. Vo verejnej časti vládneho cloudu sú identity odberateľa, vrátane externých dodávateľov projektu, prizývané ako **hosťovské účty**. Správu Microsoft Entra ID v rámci pozývania identít a priraďovania oprávnení do bezpečnostných skupín má na starosti **oddelenie správy biznis, aplikačnej a technologickej architektúry** MIRRI SR.

Pre zabezpečenie prístupu je nevyhnutné použiť autentifikátor (aplikácia alebo email) na overenie identity pomocou multifaktorovej autentifikácie (MFA). Aplikáciu pre MFA je možné nainštalovať prostredníctvom tohto odkazu:

Download and Install the Microsoft Authenticator App

Je potrebné vyplniť formulár RBAC, na základe ktorého budú vytvorené a pozvané identity do verejnej časti vládneho cloudu Azure. Tento formulár nielenže definuje prístupy, ale aj úlohy, ktoré budú mať identity v prostredí Azure. Formulár je dostupný na webovej stránke MIRRI SR, pričom zodpovednosť za správu tohto dokumentu nesie odberateľ. Ten musí zabezpečiť riadenie životného cyklu identity a informovať cloud kanceláriu MIRRI SR o všetkých zmenách.

UPOZORNENIE: Každá identita, ktorá nevykoná žiadnu aktivitu do 90 dní od prizvania, je automaticky odstránená bez upozornenia. Prizvané identity následne získavajú prístupy na Subscription podľa vyplneného formulára RBAC.

Po ukončení projektu alebo pri personálnych zmenách je povinnosťou OR požiadať o odstránenie identít ktoré nemajú mať prístup k prideleným zdrojom.

Subscription predstavuje čerpanie kreditov a organizáciu zdrojov:

- **Prístup k cloudovým službám:** Umožňuje prístup k rôznym cloudovým službám infraštruktúry Azure, ako sú virtuálne siete, virtuálne stroje, dátové úložiská, databázové riešenia a ďalšie.
- **Správa a monitorovanie:** Poskytuje nástroje na správu a monitorovanie cloudových prostredí v rámci infraštruktúry Azure, čo zabezpečuje efektívne využívanie zdrojov.
- **Riadenie prístupu a bezpečnosti:** Zabezpečuje mechanizmy na správu prístupových práv, čo umožňuje definovať špecifické oprávnenia pre jednotlivé skupiny zdrojov.
- **Štruktúrovaná správa zdrojov:** Umožňuje systematickú a efektívnu správu zdrojov pridelených rôznym projektom, tímom alebo organizačným jednotkám v rámci organizácie.
- **Izolácia zdrojov:** Zabezpečuje izoláciu zdrojov od ostatných, čím sa minimalizuje riziko neoprávneného prístupu alebo manipulácie.

Subscription sú automaticky vytvorené pre prostredia prod, dev, test a shared, pričom nasledujú číselné poradie v prípade viacerých prostredí, ktoré je potrebné izolovať.

Naming Convention (Menná konvencia) v Azure Cloud

Menná konvencia je súbor pravidiel a štandardov, ktoré určujú spôsob pomenovávania rôznych zdrojov a objektov v prostredí Azure. Cieľom menných konvencií je zabezpečiť jednotnosť, prehľadnosť a systematickosť v identifikácii a správe cloudových zdrojov, čo prispieva k efektívnejšiemu riadeniu, organizácii a monitorovaniu.

Hlavné charakteristiky mennej konvencie:

- **Jednotnosť a konzistencia**: Definuje štruktúru názvov pre rôzne typy zdrojov, ako sú virtuálne stroje, úložiská, siete a iné komponenty. Konzistentné názvy uľahčujú identifikáciu a správu zdrojov v rámci veľkých a komplexných prostredí.
- **Zrozumiteľnosť**: Pomocou jasných a jednoznačných názvov sa znižuje pravdepodobnosť nejasností a chýb pri správe zdrojov. Názvy sú zvyčajne navrhnuté tak, aby odrážali účel, typ a lokalitu zdroja.
- **Organizácia**: Umožňuje efektívne zoskupovanie a filtrovanie zdrojov na základe ich názvov. To zjednodušuje správu a reporting.
- **Automatizácia a integrácia**: Štandardizované názvy podporujú automatizované procesy a integrácie s nástrojmi a skriptami, čo zvyšuje efektivitu pri správe a nasadzovaní zdrojov

  Menná Konvencia pre Microsoft Azure

Tag (Značkovanie) v Azure Cloud

Tagging je súbor pravidiel a štandardov, ktoré umožňujú pridávať metadáta k rôznym zdrojom v Azure. Tieto značky, alebo tagy, sú vo forme kľúč-hodnota a slúžia na organizáciu, kategorizáciu a správu zdrojov v cloude. Pomocou tagov môžu správcovia systému efektívne riadiť náklady, zabezpečiť dodržiavanie predpisov, a organizovať zdroje podľa rôznych kritérií.

Hlavné charakteristiky tagovania:

- **Identifikácia a kategorizácia**: Tagy umožňujú priradiť konkrétne informácie k zdrojom, ako napríklad názov projektu, vlastník, lokalita alebo účel. Tieto informácie môžu byť nielen užitočné pri správe zdrojov, ale aj pri vykazovaní a analýze nákladov.
- **Organizácia a správa**: Tagy umožňujú vytvárať hierarchické a prispôsobené kategórie, čo zjednodušuje správu zdrojov v rámci veľkých a komplexných prostredí.
- **Automatizácia a reporting**: Pomocou tagov je možné automatizovať procesy a generovať reporty na základe preddefinovaných kritérií, čo zefektívňuje sledovanie a optimalizáciu nákladov.
- **Bezpečnosť a dodržiavanie predpisov**: Tagy môžu byť použité na sledovanie dodržiavania bezpečnostných politík a predpisov, ako aj na monitorovanie toho, či sú zdroje v súlade s organizáciou definovanými pravidlami.

  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 SR na adrese cloud@mirri.gov.sk

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.

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.
    - Odporúča sa pravidelne kontrolovať Cost Management reporty v Azure a analyzovať, či bežia všetky zdroje (napr. virtuálne stroje) tak, ako je potrebné.
    - Pri dočasných testovacích prostrediach zvážiť auto-shutdown alebo menšiu veľkosť VM, aby sa znížili náklady.
    - Ak služba už nie je potrebná, mala by sa plne odinštalovať alebo vyradiť (decommission).
    - Pravidelne vykonávať inventura tagov a kontrola orphaned resources (staré Public IP, nepoužívané diskové úložiská, vyladené NSG, apod.).
- Verejné IP adresy nie sú dostupne zo žiadneho Spoke ak je potrebná komunikácia na iné systémy ktoré sú mimo Azure prostredia, kde je potrebne definovať IP na whitelist, je potrebne kontaktovať cloud kanceláriu MIRRI SR pre dodanie IP Firewallu.

Medzi najčastejšie používane zdieľané komponenty v infraštruktúre Azure patria:

Azure Firewall

Bastion

AppGW

VPN-S2S/P2S/ExpressRoute

Private DNS Zones

DNS Private Endpoints

Centrálne komponenty predstavujú zdieľané komponenty umiestnené v centrálnom hube, pričom správa a konfigurácia týchto komponentov patrí pod zodpovednosť cloud kancelárie MIRRI SR.

Firewall je bezpečnostný komponent s vysokou dostupnosťou, umiestnený v centrálnom hube. Všetky Spoke prostredia sú pripojené do centrálneho Hub a automaticky chránené firewallom. V praxi to znamená, že ak v dotazníku nie sú definované firewall pravidlá, dané Spoke prostredie zostane nedostupné z a do vonkajšieho sveta. Je preto nevyhnutné tieto pravidlá v dotazníku zadefinovať a v prípade ich zmeny informovať cloud kanceláriu MIRRI SR**.**

Virtuálne siete sú základným stavebným prvkom cloudovéj infraštruktúry, umožňujúcim bezpečné a efektívne prepojenie rôznych cloudových služieb a prostriedkov. Každá virtuálna sieť poskytuje izolované prostredie s možnosťou definovania sieťových segmentov, smerovania a bezpečnostných pravidiel. Akékoľvek požiadavky na pridelenie alebo zmenu sieti musia byť konzultované a schválené správcom infraštruktúry MIRRI SR.

IPAM IP Address Management je systém na centralizovanú správu a alokáciu IP adries v rámci virtuálnych sietí. Umožňuje efektívne riadenie IP rozsahov, sledovanie pridelených adries a zabezpečenie konzistentnosti sieťovej infraštruktúry. V prostredí MIRRI SR sú všetky IP rozsahy prideľované a výlučne spravované v rámci centrálnej správy MIRRI SR. To zabezpečuje jednotnú adresnú schému, minimalizáciu konfliktov IP adries a centralizovanú kontrolu nad sieťovou konfiguráciou. Akékoľvek požiadavky na pridelenie alebo zmenu IP rozsahov musia byť konzultované a schválené správcom infraštruktúry MIRRI SR.

Bastion je bezpečnostný komponent, ktorý umožňuje prístup k virtuálnym strojom prostredníctvom protokolov SSH (port 22) a RDP (port 3389). Tento komponent musí byť umiestnený v zdieľanej subskripcii, keďže firewall pravidlá neumožňujú priamy prístup k tejto službe. Spoke Shared nie je chránený z a do internetu (avšak naďalej ostáva chránená interná komunikácia do centrálneho hubu), preto sa využíva výhradne len na službu Bastion as a Service, ktorá je chránená pomocou TLS a MFA. Použitie Bastion Tunnel pre Linux OS je dostupné na nasledujúcej linke.

App Gateway (AppGW) je komponent pre smerovanie webovej prevádzky na úrovni OSI Layer 7 a je umiestnený v centrálnom hube. AppGW sa nachádza v DMZ zóne a jej správa, ako aj konfigurácia, sú v kompetencii cloud kancelárie MIRRI. Pri vypĺňaní technického dotazníka je dôležité uviesť, či sú súčasťou ISVS aj webové sídla. Následne je potrebné doplniť informácie o doménových menách, portoch a TLS certifikátoch. TLS certifikáty je potrebné obstarať externe, keďže nie sú k dispozícii priamo z prostredia Azure.

Private DNS Zones je komponent pre správu domén vo virtuálnych sieťach. Všetky DNS Private Endpoints sú spravované centrálne cez cloud kanceláriu MIRRI. V prípade potreby projektu sú pre určené privátne zóny priradené pravidlá DNS contributor, ktoré umožňujú správu záznamov v rámci projektovej réžie. MIRRI SR sprostredkuje pridelenie práv a pripojenie DNS zón na požadovanú virtuálnu sieť**.**

S2S / P2S VPN je centrálny komponent poskytovaný ako manažovaná služba prostredníctvom virtuálneho WAN. To znamená, že požiadavka na pripojenie musí byť komunikovaná s cloud kanceláriou. Na základe tejto požiadavky si MIRRI SR vyžiada potrebné informácie o prepojení a následne koordinuje a zabezpečuje realizáciu pripojenia.

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 využívaná 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 odporúčanej verzie 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 cieľom zabezpečiť dodržiavanie štandardov, ktoré zahŕňajú ISO normy, ako aj najlepšie postupy od poskytovateľa cloud služieb, a to v súlade s politikami na zabezpečenie pravidiel informačnej bezpečnosti.
- Azure politiky sú 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 dostatočným 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 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 v povahe projektu umožnené.

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.
- **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.