MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Všeobecné podmienky pre pripojenie do verejnej časti vládneho cloudu

Oracle Cloud Infrastructure (OCI)

v:1.0

Popis riešenia verejnej časti vládneho cloudu v OCI

reprezentuje cloudovú infraštruktúru od spoločnosti Oracle (ďalej len, OCI), 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 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.

Globálny administrátor v Oracle Cloud Infrastructure (OCI)

Globálny administrátor má najvyššie oprávnenia v prostredí OCI 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 Identity and Access Management.
- **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.

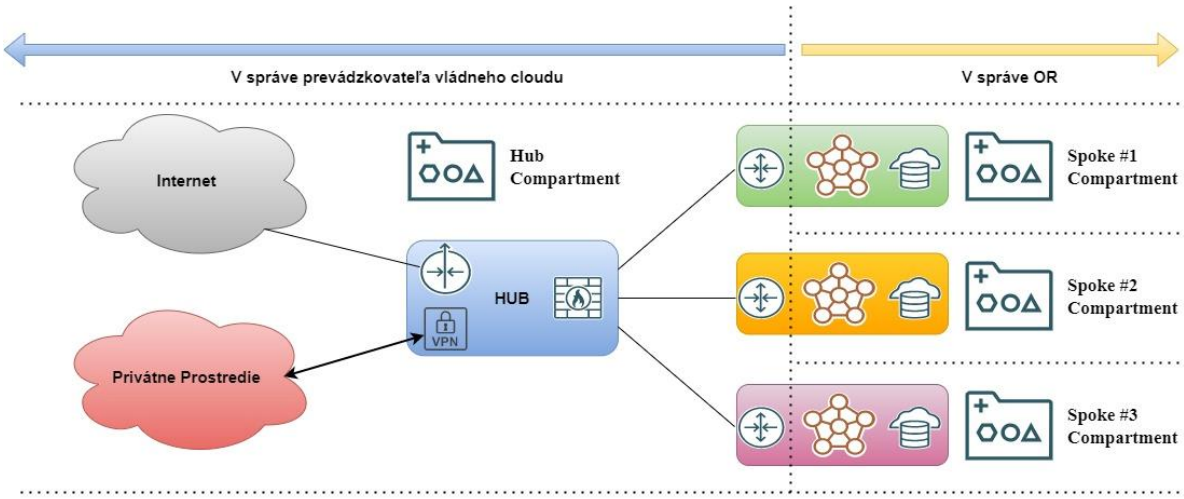
Poznámka: Globálny administrátor, je osoba zodpovedná za riadenie sekcie ITVS, má nevyhnutný prístup k celému prostrediu len v prípade narušenia bezpečnosti, kde je potrebné zabezpečiť rýchlu reakciu a riešenie problému.

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.

V rámci konceptu single-tenant sa využíva sieťová topológia „Hub & Spoke“, ktorá predstavuje architektonický model dedikovaných virtuálnych sietí. Tento model pozostáva z centrálneho hubu, ktorý je prepojený s viacerými Spoke sieťami.

Centrálny hub slúži ako kľúčový bod infraštruktúry, kde sú umiestnené kritické bezpečnostné prvky, ako napríklad firewall a ďalšie zariadenia na monitorovanie a riadenie bezpečnosti. Implementácia topológie „Hub & Spoke“ umožňuje centralizovanú kontrolu nad prístupom do a z internetu, detekciou bezpečnostných hrozieb a ochranou dát v celom prostredí OCI, vrátane virtuálnych sietí odberateľa.

Každý projekt, reprezentovaný Spoke sieťou, môže byť spravovaný a monitorovaný individuálne, pričom je v kompetencii odberateľa. Zároveň však zostávajú zachované pravidlá izolácie a bezpečného oddelenia od ostatných projektov v rámci infraštruktúry.



Obrázok 1 HA Diagram verejnej časti vládneho cloudu OCI

1. Hub:

Hub predstavuje centrálny bod infraštruktúry, ktorý spravuje konektivitu medzi externými zdrojmi a privátnym prostredím prostredníctvom Hubu. V OCI je tento model realizovaný prostredníctvom služieb ako Firewallu, VPN a APPGW, čo zabezpečuje kontrolovaný prístup k zdrojom v sieti. Riadenie sieťovej komunikácie v celom Hub prostredí je 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 svoj vlastný Compartment, čo umožňuje jednotlivým projektom alebo organizačným útvarom riadiť si svoje vlastné cloudové zdroje.

3. Virtuálne siete:

VCN poskytuje sieťové oddelenie jednotlivých projektov využívaním cloudovéj služby VCN. 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. Compartment:

Každý Spoke má svoj vlastný Compartment, ktorá je spravovaná danou OR. Compartment slúži ako logická jednotka na správu zdrojov, vrátane výpočtovej kapacity a úložiska. Každý Compartment je izolovaný, čo zaručuje nezávislosť a bezpečnosť medzi jednotlivými Spoke.

5. 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 nevyhnutné poskytnúť informácie o identitách, ktoré majú byť prizvané do vládneho cloudu v OCI. V verejnej časti vládneho cloudu sú identity orgánom riadenia (ďalej len, OR) prizývané ako hosťovské účty, čo platí aj pre externých dodávateľov projektu. MIRRI SR má na starosti správu Identity and Access Management (ďalej len, IAM) v rozsahu prizývania identít, vytvárania a pridelenia oprávnení do bezpečnostných skupín.

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 Oracle Mobile Authenticator App

Je potrebné vyplniť formulár IAM politiky, na základe ktorého budú vytvorené a spravované identity pre prístup do prostredia OCI. Tento formulár definuje nielen samotné prístupové práva, ale aj úlohy (roles), ktoré budú mať užívatelia v OCI. Formulár je dostupný na webovej stránke MIRRI SR, pričom zodpovednosť za správu prístupov nesie odberateľ. Odberateľ 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 vytvorenia alebo pozvania do OCI, môže byť automaticky deaktivovaná alebo odstránená bez predchádzajúceho upozornenia.

Tenancy a Compartment predstavuje čerpanie kreditov a organizáciu zdrojov:

- **Prístup k cloudovým službám:** Umožňuje prístup k rôznym cloudovým službám infraštruktúry OCI, 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 OCI, 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.

Compartment 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 OCI

Menná konvencia je súbor pravidiel a štandardov, ktoré určujú spôsob pomenovávania rôznych zdrojov a objektov v prostredí OCI. 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 OCI

Tag (Značkovanie) v OCI

Tagging je súbor pravidiel a štandardov, ktoré umožňujú pridávať metadáta k rôznym zdrojom v OCI. 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 OCI 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 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 už služba nie je potrebná, mala by sa plne odinštalovať alebo vyradiť (decommission).
    - Pravidelne vykonávať inventúru tagov a kontrola orphaned resources (staré Public IP, nepoužívané diskové úložiská, apod.).

- Verejné IP adresy nie sú dostupne zo žiadneho Spoke ak je potrebná komunikácia na iné systémy ktoré sú mimo OCI 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 OCI patria:

OCI Firewall

Bastion

OCI Load Balancer

VPN S2S IPSec

Internet Gateway

NAT Gateway

DRG Router

DNS Zones

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 zabezpečuje bezpečný vzdialený prístup k virtuálnym strojom prostredníctvom protokolov SSH (port 22) a RDP (port 3389)**.** Bastion ako služba (Bastion as a Service) poskytuje šifrované pripojenie chránené pomocou TLS (Transport Layer Security) a viacfaktorovej autentifikácie (MFA)**,** čím výrazne zvyšuje bezpečnosť prístupu do cloudového prostredia.

OCI Load Balancer je komponent na smerovanie webovej prevádzky na úrovni OSI Layer 7 (HTTP/HTTPS) a je umiestnený v centrálnom hub-e. Nachádza sa v DMZ zóne a jeho správa, ako aj konfigurácia, sú v kompetencii OR. Load Balancer zabezpečuje bezpečné a škálovateľné smerovanie požiadaviek na backendové servery a podporuje automatické škálovanie podľa zaťaženia. Pri vypĺňaní technického dotazníka je dôležité uviesť, či sú súčasťou ISVS aj webové aplikácie, pričom je potrebné doplniť informácie o doménových menách, portoch a TLS certifikátoch. OCI neposkytuje predinštalované TLS certifikáty, preto je nutné ich obstarať externe a následne importovať do OCI Load Balanceru, kde sú spravované cez službu OCI Certificates a aplikované na HTTPS Listener pre zabezpečenie šifrovanej komunikácie.

Internet Gateway (IGW) je komponent, ktorý umožňuje verejnú konektivitu medzi virtuálnou sieťou (VCN) a internetom. Zabezpečuje priamy prístup do a z internetu pre verejne dostupné zdroje v OCI.

NAT Gateway je služba, ktorá umožňuje odchádzajúcu komunikáciu **z** privátnej podsiete (subnetu) do internetu, pričom zabezpečuje, že zdroje v OCI zostávajú neprístupné z verejného internetu**.** Používa sa napríklad pre servery, ktoré potrebujú sťahovať aktualizácie, ale nemajú mať verejnú IP adresu.

Dynamic Routing Gateway (DRG) je virtuálny router v OCI, ktorý umožňuje privátne prepojenie medzi on-premise infraštruktúrou a OCI prostredníctvom VPN alebo FastConnect. Zabezpečuje aj prepojenie medzi viacerými virtuálnymi sieťami v rámci cloudu.

Private DNS je služba na správu doménových mien v rámci virtuálnych sietí (VCN). Všetky Private DNS záznamy sú centrálne spravované cloud kanceláriou MIRRI SR. V prípade potreby projektu sú pre pridelené privátne DNS zóny nakonfigurované politiky oprávnení, ktoré umožňujú správu DNS záznamov v rámci projektového prostredia. MIRRI SR zabezpečuje sprostredkovanie prístupu a pripojenie privátnych DNS zón k požadovanej virtuálnej sieti v OCI, čím zaručuje správne smerovanie a dostupnosť služieb v rámci izolovaných prostredí.

S2S / P2S VPN je centrálna sieťová služba poskytovaná ako manažované riešenie prostredníctvom OCI VPN Connect. To znamená, že požiadavka na pripojenie musí byť konzultovaná s cloud kanceláriou MIRRI SR. 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 OCI.

Kvóta je obmedzenie s nasledujúcimi charakteristikami:

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

Budget služba s nasledujúcimi charakteristikami:

- Slúži na sledovanie a riadenie výdavkov v rámci cloudu, 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 finančných aspektov v OCI, vrátane sledovania aktuálneho stavu výdavkov v porovnaní s definovaným rozpočtom.

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 OCI

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.
- OCI 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 OCI 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.